Naval Research Laboratory

Washington, DC 20375-5320

NRL/MR/5515--98-8304

Information Technology Division Technical Paper Abstracts 1997

Compiled By
Maryalls G. Bedford, M.S.

Sabre Systems, Inc.
Warminister, PA

Graphic Designs By
Nina D'Souza

George Washington University

Navy Center for Applied Research In Artificial Intelligence
Information Technology Division

September 30, 1998

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (*Leave Blank*)

2. REPORT DATE

September 30, 1998

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE

Information Technology Division Technical Paper Abstracts 1997

5. FUNDING NUMBERS

6. AUTHOR(S)

Maryalls G. Bedford* and Nina S. D'Souza**

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5515--98-8304

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
Arlington, VA 22217-5660

Sabre Systems, Inc.
Warminster, PA

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

*Sabre Systems, Inc., Warminster, PA
**George Washington University

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report provides abstracts for technical publications produced during 1997 by personnel of the Information Technology Division (ITD), one of the largest research and development collectives at the Naval Research Laboratory. The abstracts are organized into sections that represent the six branches with ITD: the Navy Center for Applied Research in Artificial Intelligence, Communication Systems, the Center for High Assurance Computer Systems, Transmission Technology, Advanced Information Technology, and the Center for Computational Science. Within each section, a list of branch papers published in 1995 and 1996 has also been included: abstracts for these papers may be found in prior-year editions of this report. Information on obtaining a copy of one or more of the abstracted or listed publications is provided as well.

14. SUBJECT TERMS

15. NUMBER OF PAGES

110

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT

UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT

UNCLASSIFIED

20. LIMITATION OF ABSTRACT

UL

Contents 97

This report provides abstracts for technical publications produced by ITD personnel during 1997. The abstracts are organized into sections by the ITD branch. Within each section, a list of papers published in 1995 and 1996, given ITD report number, title, and author(s), has also been included; abstracts for these papers may be found in prior-year editions of this report.

To obtain a copy of one or more of the abstracted or listed papers, contact the NCARAI librarian at 202-767-0018 (telephone); 202-767-3172 (fax); library@aic.nrl.navy.mil (e-mail); or by postal mail at

Naval Research Laboratory
Attn: NCARAI Library Code 5510
Washington, DC 20375-5337

Please give the report number, title, and author(s) of each paper desired. Additionally, the list of abstracts and a number of the papers (primarily those produced by NCARAI) are available through the WWW at URL: http://www.aic.nrl.navy.mil/papers, or by anonymous FTP to host ftp.aic.nrl.navy.mil (132.250.84.25), in the /pub/papers directory.

Introduction

The Naval Research Laboratory (NRL) is the corporate laboratory for the United States Navy, and employs more than 3, 700 civilians to conduct research and development programs in a wide range of technical disciplines. While more than 750 of NRL's employees hold doctorates, all members of the research staff participate extensively in national and international technical groups. In order to inform the research, adademic, and industrial communities of its research activites, NRL annually publishes in excess of 1,000 journal articles, technical papers, and reports.

The Information Technology Division (ITD) is one of the largest research and development collectives at NRL. ITD employs more than 220 civilian researchers organized into six branches: the Navy Center for Applied Research in Artificial Intelligence, Communication Systems, the Center for High Assurance Computer Systems, Transmission Technology, Advanced Information Technology, and the Center for Computational Science. The technical areas of expertise in ITD include :

Communications

network simulation
HF communications
communication security
communications networking

Human-Computer Interaction

visualization techniques
metrics and evaluation
speech communications
human-computer dialogue

Artificial Intelligence

intelligent simulation
adaptive control software
machine learning methods
robotic vision and control
interactive systems
intelligent decision aids
reasoning under uncertainty

Software

computer security
network security
software assurance
software specification methods
hard real time computing
adaptive software testing
information security

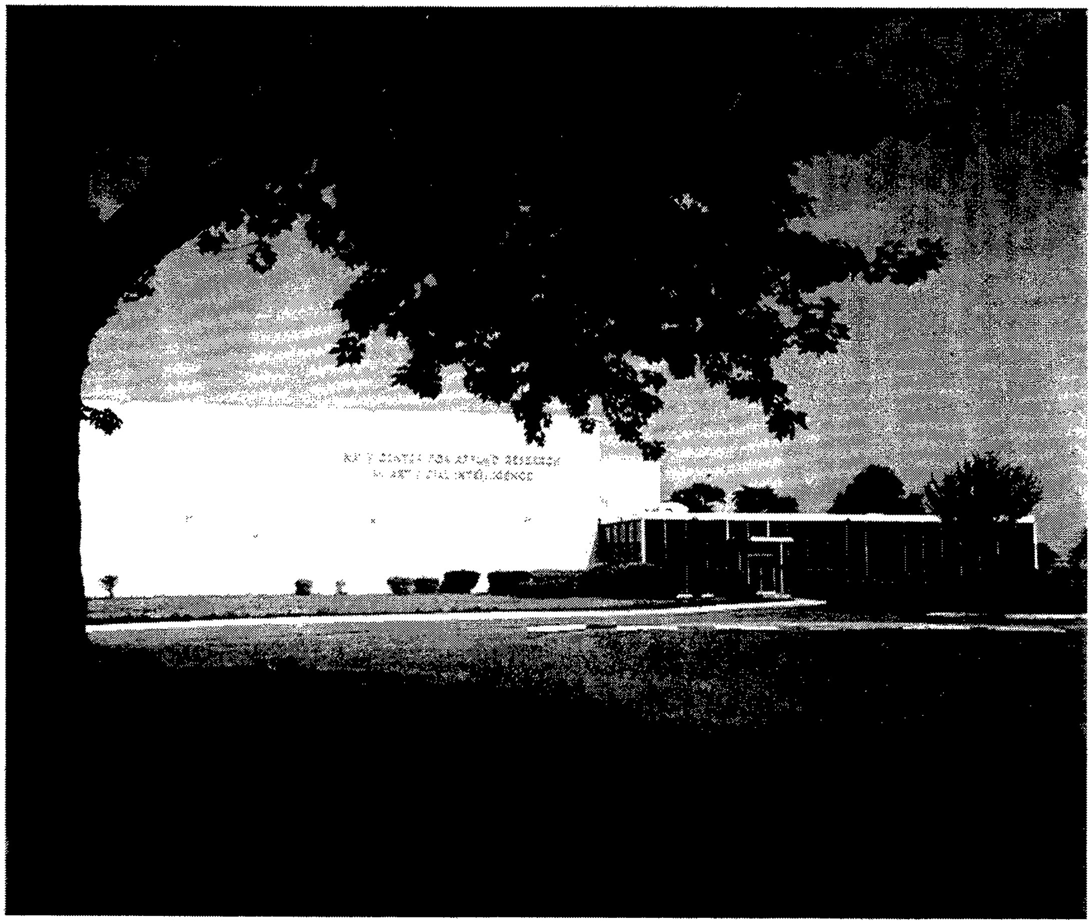
Decision Support Systems

parallel processing techniques
prototyping techniques
distributed decision support
distributed simulation

Abstracts Publication 1997

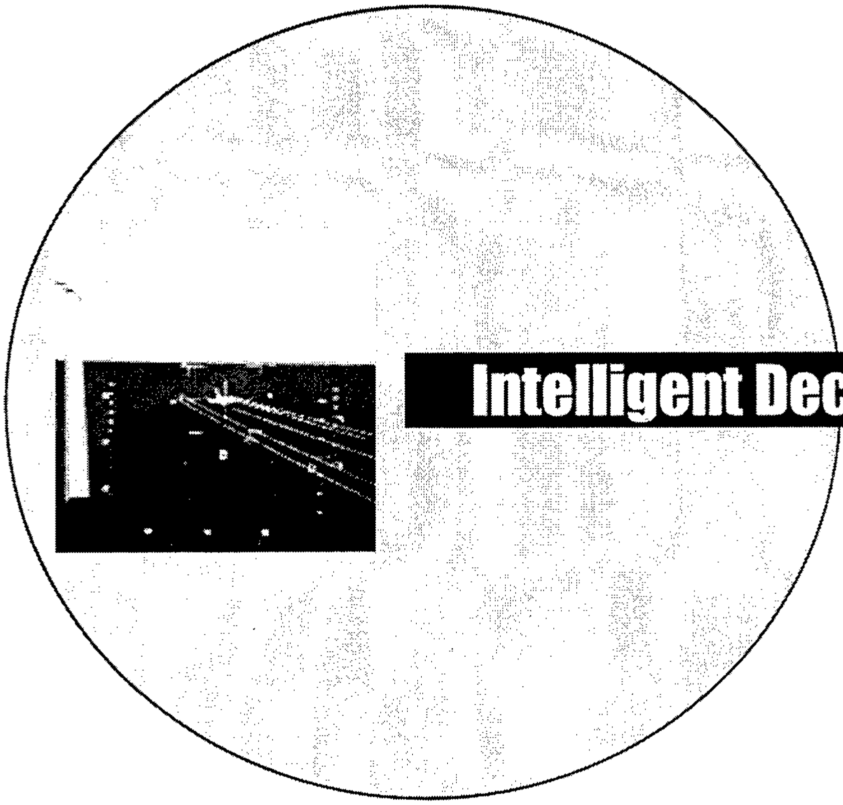
Manuscript approved September 8, 1998

Code 5510



The Navy Center For Applied Research In Artificial Intelligence (NCARAI) is engaged in research efforts designed to address the application of artificial intelligence (AI) technology and techniques critical to Navy and national concerns. The emphasis at NCARAI is the linkage of theory and application in demonstration projects that use a full spectrum of AI methods.

The technical papers and reports generated by the NCARAI document the accomplishments of projects in computational reasoning for intelligent decision aids, intelligent M4 (multi-media, multi-modal) systems, interface design and evaluation, machine learning, and sensor-based systems. Innovative basic and exploratory research in these areas are made possible by NCARAI's staff, an impressive cross section of AI talent from the Government civilian and military sectors, visiting scholars from the academic communities, and consulting scientists from various industries. An ongoing seminar series, featuring notable scientists and scholars from around the country and abroad, provides an excellent forum to exchange information and maintain awareness of current developments.



Intelligent Decision Aids

INTELLIGENT DECISION AIDS

Title: Learning to Refine Case Libraries: Initial Results
Authors: David W. Aha and Leonard A. Breslow
E-mail Address: aha@aic.nrl.navy.mil or breslow@aic.nrl.navy.mil
Citation: In D. Wettschereck & D. W. Aha (Eds.) ECML-97 MLNet Workshop Notes: Case-Based Learning: Beyond Classification of Feature Vectors
Date: 1997
Report No.: AIC-97-003

Abstract

Commercial case-based reasoning (CBR) systems are advertised for their ease of use. However, designing large case libraries that have good performance is difficult. CBR vendors provide guidelines for designing libraries, but they are challenging to apply. We describe promising initial empirical results for an inductive approach that revises case libraries to increase their conformance with design guidelines.

Title: Refining Conversational Case Libraries.
Authors(s): David W. Aha and Leonard A. Breslow
E-mail Address: aha@aic.nrl.navy.mil or breslow@aic.nrl.navy.mil
Citation: Proceedings of the Second International Conference on Case-Based Reasoning, Providence, RI: Springer-Verlag, pp267-278
Date: 1997
Report No.: AIC-97-004

Abstract

Conversational case-based reasoning (CBR) shells (e.g., Inference's CBR Express) are commercially successful tools for supporting the development of help-desk and related applications. In contrast to rule-based expert systems, they capture knowledge as cases rather than more problematic rules, and they can be incrementally extended. However, rather than eliminate the knowledge engineering bottleneck, they refocus it on case engineering, the task of carefully authoring cases according to library design guidelines to ensure good performance. Designing complex libraries according to these guidelines is difficult; software is needed to assist users with case authoring. We describe an approach for revising case libraries according to design guidelines, its implementation in Clire, and empirical results showing that, under some conditions, this approach can improve conversational CBR performance.

Title: NACODAE: Navy Conversational Decision Aids Environment
Author(s): David W. Aha and Leonard A. Breslow
E-mail Address: aha@aic.nrl.navy.mil or breslow@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-018

Abstract

This report documents NACODAE, the Navy Conversational Decision Aids Environment being developed at the Navy Center for Applied Research in Artificial Intelligence (NCARAI), which is a branch of the Naval Research Laboratory. NACODAE is a software prototype that is being developed under the *Practical Advances in Case-Based Reasoning* project, which is funded by the Office for Naval Research, for the purpose of assisting Navy and other DoD personnel in decision aids tasks such as system maintenance, operational training, crisis response planning, logistics, fault diagnosis, target classification, and meteorological nowcasting. Implemented in Java, NACODAE can be used on any machine containing a Java virtual machine (e.g., Pcs, Unix). This document describes and exemplifies NACODAE's capabilities. Our goal is to transition this tool to operational personnel, and to continue its enhancement through user feedback and by testing recent research advances in case-based reasoning and related areas.

Title: A Model-Based Approach for Supporting Dialogue Inferencing in a Conversational Case-Based Reasoner
Author(s): David W. Aha and Tucker Maney
E-mail Address: aha@aic.nrl.navy.mil or maney@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-023

Abstract

Conversational case-based reasoning (CCBR) is a form of interactive case-based reasoning where users input a partial problem description (in text). The CCBR system responds with a ranked solution display, which lists the solutions of stored cases whose problem descriptions best match the user's, and a ranked question display, which lists the unanswered questions in these cases. Users interact with these displays, either refining their problem description by answering selected questions, or selecting a solution to apply. CCBR systems should support dialogue inferencing; they should infer answers to questions that are implied by the problem description. Otherwise, questions will be listed that the user believes they have already answered. The standard approach to dialogue inferencing allows case library designers to insert rules that define implications between the problem description and unanswered questions. However, this approach imposes substantial knowledge engineering requirements. We introduce an alternative approach whereby an

intelligent assistant guides the designer in defining a model of their case library, from which implication rules are derived. We detail this approach, its benefits, and explain how it can be supported through an integration with Parka-DB, a fast relational database system. We will evaluate our approach in the context of our CCBR system, named NaCoDAE.

Title: The Omnipresence of Case-Based Reasoning in Science and Application
Author(s): David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-024

Abstract

A surprisingly large number of research disciplines have contributed towards the development of knowledge on lazy problem solving, which is characterized by its storage of ground cases and its demand driven response to queries. Case-based reasoning (CBR) is an alternative, increasingly popular approach for designing expert systems that implements this approach. This paper lists pointers to some contributions in some related disciplines that offer insights for CBR research. We then outline a small number of Navy applications based on this approach that demonstrate its breadth of applicability. Finally, we list a few successful and failed attempts to apply CBR, and list some predictions on the future roles of CBR in applications.

Intelligent M4 Systems

Abstracts Publication 1997

Title: The Functionality of It-clefts in Selected Discourses: The Message in the Medium
Author(s): Dennis Perzanowski and John Gurney
E-mail Address: dennisp@aic.nrl.navy.mil
Citation: WORD, v48, n2, August 1997, pp207-236
Date: August 1997
Report No.: AIC-97-019

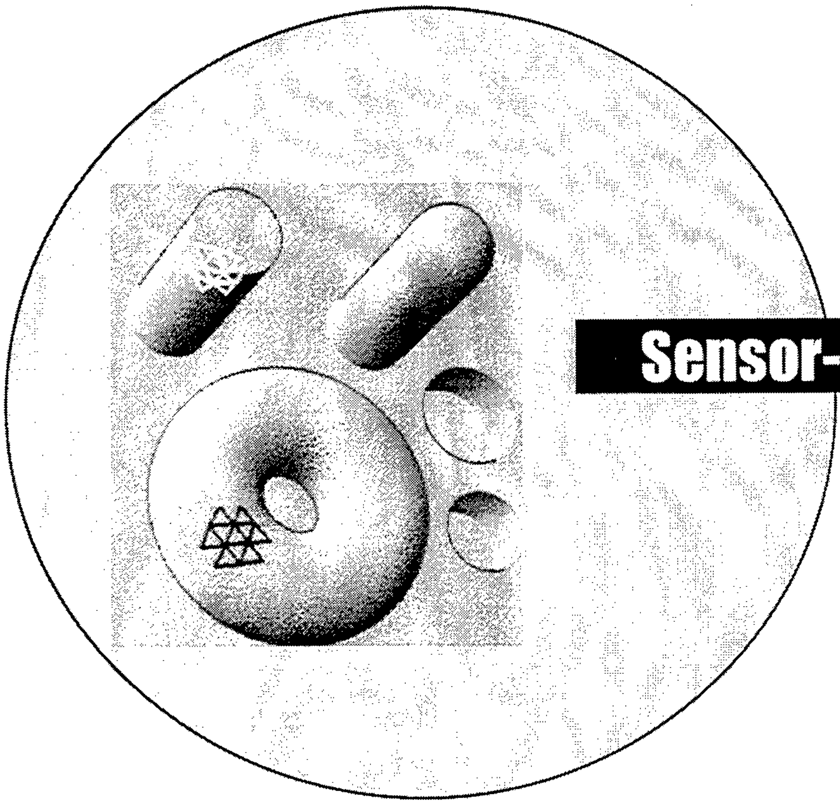
Abstract

Information in a discourse can be obtained by analyzing several different linguistic properties of the discourse. Various syntactic and semantic triggers provide clues to the complex informational structure of a discourse. For the purposes of this investigation, we selected several discourses taken from a series of wire service messages dealing with terrorist incidents that occurred in Central America from 1989 to 1991. The corpus is known as the "MUC-3" corpus. Because of their inferential properties, we identified it-cleft constructions in the corpus. We argue that, despite their rarity in the corpus under investigation, it-clefts provide additional information, and do not just contrast or emphasize focused linguistic material, such as noun or prepositional phrases. By substituting so-called "normal" word order, or SVO paraphrases, for the it-clefts in the messages, we determined what information the it-cleft sentences provided in the discourse. Our investigation reveals that, as a subset of the information that can be obtained in a discourse, it-clefts can be used to avoid conflicting or differing interpretations inherent in their SVO paraphrases, thereby minimizing possible confusion regarding the interpretation of what the author is trying to communicate. In some cases the speaker/writer's point of view or attitude about the subject matter being discussed is also revealed. For example, we show how a focused generic noun phrase in an it-cleft sentence provides a clearer statement of the author's intended meaning.

Title: Natural Language in Four Spatial Interfaces
Author(s): Kenneth Wauchope, Stephanie Everett, Dennis Perzanowski, and Elaine Marsh
E-mail Address: wauchope@aic.nrl.navy.mil or severett@aic.nrl.navy.mil or dennisp@aic.nrl.navy.mil or marsh@aic.nrl.navy.mil
Citation: Proceedings of the Fifth Conference on Applied Natural Language Processing, Association for Computational Linguistics, March 31 - April 3, 1997, pp8-11
Date: March 31 - April 3, 1997
Report No.: AIC-97-020

Abstract

We describe our experiences building spoken language interfaces to four demonstration applications all involving 2- or 3-D spatial displays or gestural interactions: an air combat command and control simulation, an immersive VR tactical scenario viewer, a map-based air strike simulation tool with cartographic database, and a speech/gesture controller for mobile robots.



Sensor-Based Systems

SENSOR-BASED SYSTEMS

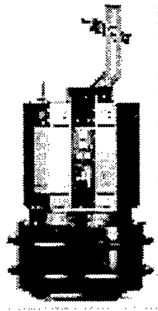
Title: Moving-Correlation-Code Triagulation Range Imaging

Author(s): Frank Pipitone and Ralph Hartley
E-mail Address: pipitone@aic.nrl.navy.mil or hartley@aic.nrl.navy.mil

Citation: Proceedings of SPIE: Sensors and Controls for Advanced Manufacturing, October 14-15, 1997, Pittsburgh, PA
Date: October 1997
Report No.: AIC-97-028

Abstract

A new method is described for obtaining accurate range images at high speed in a low-cost instrument. A prototype has been built and tested, and a patent application submitted. The method resembles grid-coding in that a camera and a stripe projector are directed at a scene, but the projector is different. It consists of a thin light source (xenon tube and slit) on the axis of a turntable, and a binary mask conforming to a cylinder coaxial with this. The mask has alternate black and clear stripes parallel to the axis. It forms a DeBruijn sequence, i.e., a sequence in which all possible sub-sequences of given length n occur. No lens is used, deliberately smoothing the resulting illumination. In operation, the turntable rotates, and six consecutive images are taken at uniform intervals. A given pixel records six consecutive samples of a scene point. This six-vector, when normalized to unity to accommodate reflectance variations, is unique to the place in the sequence from which it came. Thus we can compute the position in 3-space of the surface point at which the pixel is looking. Observed accuracy is .1 millimeter at 30 centimeters range.



Machine Learning

MACHINE LEARNING

Title: Extending Local Learners with Error-Correcting Output Codes
Author(s): Francesco Ricci and David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-001

Abstract

Error-correcting output codes (ECOCs) represent classes with a set of output bits, where each bit encodes a binary classification task corresponding to a unique partition of the classes. Algorithms that use ECOCs learn the function corresponding to each bit, and combines them to generate class predictions. ECOCs can reduce both variance and bias errors for multiclass classification tasks when the errors made at the output bits are not correlated. They work well with global (e.g., C4.5) but not with local (e.g., nearest neighbor) classifiers because the latter use the same information to predict each bit's value, which yields correlated errors. This is distressing because local learners are excellent classifiers for some types of applications. We show that the output bit errors of local learners can be decorrelated by selecting different features for each bit. This yields bit-specific distance functions, which causes different information to be used for each bit's prediction. We present promising empirical results for this combination of ECOCs, nearest neighbor, and feature selection. We also describe modifications to racing algorithms for feature selection that improve their performance in this context.

Title: Case-Based Learning: Beyond Classification of Feature Vectors
Author(s): David W. Aha and Dietrich Wettschereck
E-mail Address: aha@aic.nrl.navy.mil
Citation: In Proceedings of the Ninth European Conference on Machine Learning. Prague: Springer, pp329-336
Date: 1997
Report No.: AIC-97-002

Abstract

The dominant theme of case-based research at recent ML conferences has been on classifying cases represented by feature vectors. However, other useful tasks can be targeted, and other representations are often preferable. We review the recent literature on case-based learning, focusing on alternative performance tasks and more expressive case representations. We also highlight topics in need of additional research.

Title: ECML-97 MLNet Workshop Notes--Case-Based Learning: Beyond Classification of Feature Vectors
Author(s): Dietrich Wettschereck and David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: 1997 European Conference on Machine Learning MLNet Workshop, Prague, Czech Republic, April 26, 1997
Date: April 26, 1997

Report No.: AIC-97-005

Abstract

This collection contains the ten papers presented at the 1997 European Conference on Machine Learning MLNet Workshop entitled "Case-Based Learning: Beyond Classification of Feature Vectors." This workshop took place on April 26, 1997 in Prague, Czech Republic. Information on this workshops' objectives and other details can be found at either of the following two World Wide Web pages:

http://www.aic.nrl.navy.mil/~aha/ecml97-wkshp/
http://nathan.gmd.de/persons/dietrich.wettschereck/ecml97ws.html

---

Title: Magellan: A Mobile Robot Integrating Place Recognition, Continuous Localization, and Adaptive Navigation
Author(s): Brian Yamauchi, Alan Schultz, William Adams, Patrick Langley, and John Grefenstette
E-mail Address: yamauchi@aic.nrl.navy.mil or schultz@aic.nrl.navy.mil or adams@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-006

This report has no absract.

Title: Levels of Evolution for Control Systems
Author(s): John J. Grefenstette
E-mail Address: library@aic.nrl.navy.mil
Citation: In Genetic Algorithms in Engineering Systems, P.J. Fleming and A.M.S. Zalzala (Eds.), Peter Peregrinus Press, 1997.
Date: 1997
Report No.: AIC-97-007

Abstract

Evolutionary algorithms (EAs) are general purpose search and learning methods that can be applied to a variety of problems related to control systems. This article focuses on the range of representation levels at which evolutionary algorithms can be applied to control systems, including evolving control parameters, evolving complex control structures, and evolving control rules. The discussion also outlines the use of evolutionary algorithms for testing intelligent control systems. In this case, the EA is used to identify weaknesses in a control system by searching for challenging test cases.

Title: Summary of the 1995 AAAI Fall Symposium on Adaptation of Knowledge for Reuse
Author(s): David W. Aha and A. Ram
E-mail Address: aha@aic.nrl.navy.mil
Citation: AI Magazine, v17, n1, pp83-84
Date: 1997
Report No.: AIC-97-008

This article has no abstract.

Title: Editorial: Lazy Learning
Author(s): David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: In Artificial Intelligence Review, v11,n1-5, 1997, pp7-10
Date: 1997
Report No.: AIC-97-009

This published article has no abstract.

Title: Continuous Localization in Changing Environments
Author(s): Kevin Graves, William Adams, and Alan Schultz
E-mail Address: adams@aic.nrl.navy.mil or schultz@aic.nrl.navy.mil
Citation: Proceedings of the International Symposium on Computational Intelligence in Robotics and Automation, July 1997
Date: July 1997
Report No.: AIC-97-010

Abstract

Continuous localization is a technique that allows a robot to maintain an accurate estimate of its location by performing regular, small corrections to its odometry. Continuous localization uses an evidence grid representation, a common representation scheme that is used by other map-dependent processes, such as path planning. Although techniques exist for building evidence grid maps, most are not adaptive to changes in the environment. In this research, we extend the continuous localization technique by adding a learning component. This allows continuous localization to update the long-term map (evidence grid) with current sensor readings. Results show that the addition of the learning behavior to continuous localization allows the system to adapt to changes in its environment without a loss in its ability to remain localized. This system was tested on a Nomad 200 mobile robot

---

Title: ARIEL: Autonomous Robot for Integrated Exploration and Localization
Author(s): Brian Yamauchi, Alan Schultz, William Adams, Kevin Graves, John Grefenstette, and Dennis Perzanowski
E-mail Address: yamauchi@aic.nrl.navy.mil or schultz@aic.nrl.navy.mil or adams@aic.nrl.navy.mil or dennisp@aic.nrl.navy.mil
Citation: Proceedings of the National Conference on Artificial Intelligence, July 1997
Date: July 1997
Report No.: AIC-97-011

Abstract

In order for a robot to add its perceptions to a map, it needs to know its location, but in order for a robot to determine its location, it often needs a map. This is a central dilemma in robot exploration. Robots often use dead reckoning to estimate their position without a map, but wheels slips and internal linkages may be imprecise. These errors accumulate over time, and the robot's position estimate becomes increasingly inaccurate.

We have addressed this problem in ARIEL. ARIEL uses frontier-based exploration (Yamauchi 1997) to navigate to unexplored space and to map the territory that it perceives and continuous localization (Schultz, Adams, and Grefenstette 1996) to maintain an accurate estimate of its position at all times.

ARIEL has been implemented on a Nomad 200 mobile robot equipped with sonar, infrared, and laser range sensors. ARIEL runs on a SPARCstation 20 and communicates with the robot's onboard Pentium processor via radio ethernet. This system has been used to explore real-world office environments. We will demonstrate ARIEL at the AAAI-97 Robot Exhibition.

We are also interested in using genetic algorithms to automatically learn behaviors for controlling mobile robots, and we will be demonstrating some of those learned behaviors at the Exhibition.

Title: Cognitive Model of Learning to Navigate
Author(s): Diana F. Gordon and D. Subramanian
E-mail Address: gordon@aic.nrl.navy.mil
Citation: Proceedings of the Nineteenth Annual Conference of the Cognitive Science Society, Laurence Eribaum Publishers
Date: 1997
Report No.: AIC-97-012

Abstract

Our goal is to develop a cognitive model of how humans acquire skills on complex cognitive tasks. We are pursuing this goal by designing computational architectures for the NRL Navigation task, which requires competent sensorimotor coordination. In this paper, we analyze the NRL Navigation task in depth. We then use data from experiments with human subjects learning this task to guide us in constructing a cognitive model of skill acquisition for the task. Verbal protocol data augments the black box view provided by execution traces of inputs and outputs. Computational experiments allow us to explore a space of alternative architectures for the task, guided by the quality of fit to human performance data.

Title: Using Problem Generators to Explore the Effects of Epistasis
Author(s): Kenneth A. De Jong, Mitchell Potter, and William M. Spears
E-mail Address: dejong@aic.nrl.navy.mil or potter@aic.nrl.navy.mil or spears@aic.nrl.navy.mil
Citation: Proceedings of the Seventh International Conference on Genetic Algorithms, Morgan Kaufmann, July 1997, pp338-345
Date: July 1997
Report No.: AIC-97-013

Abstract

In this paper, we develop an empirical methodology for studying the behavior of evolutionary algorithms based on program generators. We then describe three generators which are particularly well suited for studying the effects of epistasis on the performance of EAs. Finally, we illustrate the use of these ideas in a preliminary exploration of the effects of epistasis on simple GAs.

Title: A Frontier-Based Approach for Autonomous Exploration
Author(s): Brian Yamauchi
E-mail Address: yamauchi@aic.nrl.navy.mil
Citation: Proceedings of the 1997 IEEE International
Symposium on Computational Intelligence in Robotics and Automation,
Monterey, CA, IEEE Computer Society, pp146-151
Date: July 1997
Report No.: AIC-97-014

Abstract

Frontier-based exploration directs mobile robots to regions on the boundary between unexplored space and space that is known to be open. Previously, we have demonstrated that frontier-based exploration can be used to map indoor environments containing both open and cluttered spaces, where walls and obstacles may be in arbitrary orientations. In this paper, we show how frontier-based exploration can be extended to multiple robots. In our approach, robots share perceptual information, but maintain separate global maps, and make independent decisions about where to explore. This approach enables robots to make use of information from other robots to explore more effectively, but it also allows the team to be robust to the loss of individual robots. We have implemented our multi-robot exploration system on real robots, and we demonstrate that they can explore and map office environments as a team.

Title: Reinforcement Learning Through Evolutionary Computation
Author(s): D. Moriarty, Alan Schultz, and John Grefenstette
E-mail Address: schultz@aic.nrl.navy.mil
Citation: Submitted to the Journal on Artificial Intelligence Research (JAIR),
May 1997
Date: May 1997
Report No.: AIC-97-015

Abstract

This article characterizes the evolutionary algorithm approach to reinforcement learning in relation to the more standard, temporal difference methods. We describe several research issues in reinforcement learning and discuss similarities and differences in how they are addressed by the two methods. A short survey of evolutionary reinforcement learning systems and their successful applications is also presented.

Title: Asimovian Adaptive Agents
Author(s): Diana Gordon
E-mail Address: gordon@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-016

Abstract

How can we guarantee that software and robotic agents will behave as we require (as in Asimov's laws), even after learning and adaptation? Formal verification is the answer. Nevertheless, formal verification is computationally costly for agents to perform at run-time. This paper presents a priori proofs that certain learning operators are guaranteed ``safe" to perform, i.e., they will not violate specified classes of desirable properties (laws). The paper also provides counterexamples that show that other learning operators cannot be guaranteed safe for these property classes.

Title: User's Guide to Samuel 97: An Evolutionary System
Author(s): John Grefenstette
E-mail Address: library@aic.nrl.navy.mil
Citation: Internal Report
Date: August 1997
Report No.: AIC-97-017

Abstract

SAMUEL is a machine learning program that uses genetic algorithms and other competition-based heuristics to solve sequential decision problems. The system actively explores the space of alternative decision policies in simulation, and modifies its candidate policies based on this experience. Policies are represented as condition-action rules. The genetic algorithm in SAMUEL includes the standard methods of fitness-directed reproduction of rulebases, random mutation, and crossover. In addition, SAMUEL features several Lamarckian operators that modify decision rules on the basis of observed interaction with the task environment. SAMUEL has been used to learn decision policies for behaviors such as navigation and collision avoidance, tracking, and herding, for robots and other autonomous vehicles. SAMUEL also includes mechanisms to allow coevolution of multiple behaviors simultaneously. SAMUEL incorporates a convenient language for the decision rules, making it possible for the user to initialize the learning system with existing knowledge. SAMUEL is written in ANSI C and runs under the UNIX operating system. The visualization tool is written in Java, and allows output to be viewed with any Java-enabled browser or applet viewer.

Title: Integrating Exploration and Localization for Mobile Robots
Author(s): Brian Yamauchi, Alan Schultz, and William Adams
E-mail Address: yamauchi@aic.nrl.navy.mil or schultz@aic.nrl.navy.mil or adams@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-021

Abstract

Exploration and localization are two of the capabilites necessary for mobile robots to navigate robustly in unknown environments. A robot needs to explore

in order to learn the structure of the world, and a robot needs to know its own localization in order to make use of its acquired spatial information. However, a problem arises with the integration of exploration and localization. A robot needs to know its own localization in order to add new information to its map, but a robot may also need a map to determine its own location. We have addressed this problem with ARIEL, a mobile robot system that combines frontier-based exploration with continuous localization. ARIEL is capable of exploring and mapping an unknown environment while maintaining an accurate estimate of its position at all times. In this paper, we describe frontier-based exploration and continuous localization, and we explain how ARIEL integrates these techniques. Then we show results from experiments performed in the exploration of a real-world office hallway environment. These results demonstrate that maps learned using exploration without localization suffer from substantial dead reckoning errors, while maps learned by ARIEL avoid these errors and can be used for reliable exploration and navigation.

Title: Frontier-Based Exploration Using Multiple Robots
Author(s): Brian Yamauchi
E-mail Address: yamauchi@aic.nrl.navy.mil
Citation: Submitted to The Second International Conference on Autonomous Agents (Agents '98), Minneapolis, MN, 1998
Date: 1997
Report No.: AIC-97-022

Abstract

Frontier-based exploration directs mobile robots to regions on the boundary between unexplored space and space that is known to be open. Previously, we have demonstrated that frontier-based exploration can be used to map indoor environments containing both open and cluttered spaces, where walls and obstacles may be in arbitrary orientations. In this paper, we show how frontier-based exploration can be extended to multiple robots. In our approach, robots share perceptual information, but make maintain separate global maps, and make independent decisions about where to explore. This approach enables robots to make

Title: Bias, Variance, and Error Correcting Output Codes for Local Learners
Author(s): David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-025

Abstract

This paper focuses on a bias variance decomposition analysis of a local learning algorithm, the nearest neighbor classifier, that has been extended with error correcting output codes. This extended algorithm often considerably reduces the 0-1 (i.e., classification) error in comparison with nearest neighbor

(Ricci & Aha, 1997). The analysis presented here reveals that this performance improvement is obtained by drastically reducing bias at the cost of increasing variance. We also show that, even in classification problems with few classes (m<=5), extending the codeword length beyond the limit that assures column separation yields an error reduction. This error reduction is not only in the variance, which is due to the voting mechanism used for error-correcting output codes, but also in the bias.

Title: Mobile Robot Exploration and Map-Bulding With Continuous Localization
Author(s): Brian Yamauchi, Alan Schultz, and Willam Adams
E-mail Address: yamauchi@aic.nrl.navy.mil or schultz@aic.nrl.navy.mil or adams@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-026

Abstract

Our research addresses how to integrate exploration and localization for mobile robots. A robot exploring and mapping an unknown environment needs to know its own location, but it may need a map in order to determine that location. In order to solve this problem, we have developed ARIEL, a mobile robot system that combines frontier-based exploration with continuous localization. ARIEL explores by navigating to frontiers, regions on the boundary between unexplored space and space that is known to be open. ARIEL finds these regions in the occupancy grid map that it builds as it explores the world. ARIEL localizes by matching its recent perceptions with the information stored in the occupancy grid. We have implemented ARIEL in a real-world office environment. We present quanitative results that demonstrate that ARIEL can localize accurately while exploring, and thereby build accurate maps of its environment.

Title: Empirical Observations on the Roles of Crossover and Mutation
Author(s): Annie S. Wu, Robert K. Lindsay, and Rick L. Riolo
E-mail Address: aswu@aic.nrl.navy.mil
Citation: Proceedings of the 7th International Conference on Genetic Algorithms, July 1997, East Lansing, MI, pp362-369
Date: July 1997
Report No.: AIC-97-029

Abstract

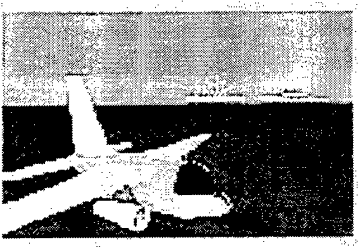
There is a great deal of information to be gained from studying the details within a GA run. This paper investigates the roles of crossover and mutation by observing the actions and effects of individual occurrences of each genetic

operation. The observations are compared with some of the common expectations of these operators.

Title: An Evolutionary Computation Model of Emerging Virus Diseases
Author(s): John J. Grefenstette, Donald S. Burke, Kenneth A. De Jong, Connie L. Ramsey and Annie S. Wu
E-mail Address: dejong@aic.nrl.navy.mil or ramsey@aic.nrl.navy.mil or aswu@aic.nrl.navy.mil
Citation: Internal Report
Date: 1997
Report No.: AIC-97-030

Abstract

A computational model of virus evolution has been developed that enables the study of fundamental questions concerning the evolved structure of the viral genotypes, the dynamics of cross-species infection, and the role of alternative recombination strategies exhibited by viruses. The ``Virtual Virus" (VIV) model consists of populations of hundreds to thousands of variable length virtual virus genomes that replicate, mutate, recombine, and evolve. Each virus genome is composed of an artificial polynucleotide string in which arbitrary ``nucleotide" triplets encode English letters rather than amino acids, and in which sequences are translated into words or phrases, rather than into polypeptides or proteins. The three word/phrases ``COREPROTEIN," ``POLYMERASE," and ``ENVELOPE," which can be present in any order on the string, together comprise the selected phenotype. Run-on and overlapping reading frames are permitted. Fitness is assigned to each string according to the encoded spelling score. Perfect spelling of all words is assigned a fitness of 1.0, while gibberish is assigned a fitness score of 0.0. Redundancies and non-coding regions are not directly scored, but string brevity is rewarded with higher fitness. Probability of replication at each generation is directly related to string fitness. VIV populations seeded with random strings regularly evolve terse, high spelling score genomes within a few hundred to a thousand generations. Sub-population phylogenies and individual ancestries can be recalled, displayed, and analyzed with a JAVA-based visualization tool. By systematically varying evolutionary operators in the VIV model we observed several reproducible features relevant to the evolution and emergence of biological viruses: (1) adaptation (fitness slope) proceeds most rapidly at mutation rates close to one per genome, and falls off rapidly at rates either higher or lower than unity (2) when added to mutation, recombination in any form speeds adaptation, and (3) homologous recombination is superior to random cross-over recombination. The VIV model is designed so that it can be conveniently modified to incorporate a variety of additional evolutionary operators, such as genome segmentation, genomic secondary structures, insertions and deletions, and feed-back loops and hypercycles. VIV can also be adapted to model the evolution and emergence of mutable computer virus threats.



Interface Design & Evaluation

Abstracts Publication 1997

Title: Interruption of People in Human-Computer Interaction: A General Unifying Definition of Human Interruption and Taxonomy
Author(s): Daniel C. McFarlane
E-mail Address: mcfarlan@itd.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5510--97-9870
Date: December 31, 1997
Report No.: AIC-97-027

Abstract

User-interruption in human-computer interaction (HCI) is an increasingly important problem. Many of the useful advances in intelligent and multitasking computer systems have the significant side effect of greatly increasing user-interruption. This previously innocuous HCI problem has become critical to the successful function of many kinds of modern computer systems. Unfortunately, no HCI design guidelines exist for solving this problem. In fact, theoretical tools do not yet exist for investigating the HCI problem of user-interruption in a comprehensive and generalizable way. This report asserts that a single unifying definition of user-interruption and the accompanying practical taxonomy would be useful theoretical tools for driving effective investigation of this crucial HCI problem. These theoretical tools are constructed here. A comprehensive analysis is conducted through the existing literature. Theoretical constructs from several relevant but diverse fields are identified and discussed. A unifying definition of user-interruption is synthesized. This new definition is supported with an array of postulates, assertions, and a taxonomy of human interruption to facilitate its practical application.

Title: Performance Based Design of a New Virtual Locomotion Control
Author(s): James N. Templeman
E-mail Address: templema@itd.nrl.navy.mil
Citation: NATO RSG-28 Human Factors Issues in Virtual Reality Technologies Conference Proceedings
Date: 1997
Report No.: AIC-97-031

Abstract

The ability to simulate walking around in the environment is a key element missing from most of today's joint forces simulations. A number of sensor-based techniques are widely used to maneuver through Virtual Environments but they introduce artifacts into the interaction. Mechanical motion platforms have also been applied to surmount these difficulties, but they tend to exhibit different but equally troublesome side effects of their own. This paper examines the interrelationships between virtual motion control and other critical actions soldiers need to perform in VE. The goal is to

allow the user to maneuver through VE in as similar a manner as possible to walking through the real world. If the interactions between different controls and sensory feedback can be made comparable to the interaction between actions in the real world, then there is hope for constructing an effective new technique. Human performance requirements are viewed from an analytical standpoint: pointing out the interactions between a full set of virtual controls that would allow the user to act, sense, and react to their environment. Candidate solutions are discussed as the analysis is developed. This has lead us to a promising new design for sensor-based virtual locomotion called Gaiter, introduced in this paper.

Title: Verbal vs. Computer Acknowledgments in High Workload Team Communications
Author(s): Astrid Schmidt-Nielsen, Kay G. Schulze, and Lisa B. Achille
E-mail Address: schmidtn@aic.nrl.navy.mil
Citation: Abstracts of the Psychonomic Society, 2, 36 (Abstract).
Date: 1997
Report No.: AIC-97-032

Abstract

Using a team decision making task that requires collecting information from several sources (a simulated Navy task with a high communication load), we invesitagated the changes in decision-making performance when some of the information usually conveyed verbally is conveyed by computer. Decison making performance will be compared across conditions when all communication is human-to-human and when some of the commmunication is either human-to-computer, computer-to-human, or computer-to-computer.

Title: Perceptually Based Scheduling Algorithms for Real-time Synthesis of Complex Sonic Environments
Author(s): Hesham Fouad, James K. Hahn, and James A. Ballas
E-mail Address: ballas@itd.nrl.navy.mil
Citation: The Fourth International Conference on Auditory Display (ICAD ;97), Palo Alto, CA, Nov. 2-5, 1997
Date: November 2-5, 1997
Report No.: AIC-97-033

Abstract

In this paper, we present a technique for managing overload conditions that occur when computational resources are not sufficient to evaluate all the active sound sources in a Virtual Environment. A real-time scheduling strategy is introduced which degrades less important sound sources so that resource constraints are met. Finally, scheduling algorithms are considered based on their effect on listeners' perception of the resultant sound quality.

1996 PUBLICATIONS

AIC-96-001 A Collaborative Model of Feedback in Human-Computer Interaction, *Manuel A. Pérez-Quiñones and John L. Sibert*

AIC-96-002 Negotiating User-Initiating Cancellation and Interruption Requests, *Manuel A. Pérez-Quiñones and John L. Sibert*

AIC-96-003 Rejection with Multilayer Neural Networks: Screening Image Data, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-96-004 Greedy Utile Suffix Memory for Reinforcement Learning with Perceptually-Aliased States, *Leonard A. Breslow*

AIC-96-005 Cooperative Bayesian and Case-Based Reasoning for Solving Multiagent Planning Tasks, *David W. Aha and Liwu W. Chang*

AIC-96-006 A Review and Comparative Evaluation of FeatureWeighting Methods for Lazy Learning Algorithms, *Dietrich Wettschereck, David W. Aha, and Takao Mohri*

AIC-96-007 Continuous Localization Using Evidence Grids, *Alan C. Schultz, William Adams, and John J. Grefenstette*

AIC-96-008 Case-Based Retrieval and Indexing Using a Bayesian Network Model, *Liwu W. Chang and Patrick R. Harrison*

AIC-96-009 A NN Algorithm for Boolean Satisfiability Problems, *William M. Spears*

AIC-96-010 Content Analysis of Communication in a Hierarchical Navy Team, *Lisa B. Achille and Kay G. Schulze*

AIC-96-011 The Message in the Medium: On the Functionality of It-clefts in Selected Discourses, *Dennis Perzanowski and John Gurney*

AIC-96-012 Models of Action Selection Learning, *Diana Gordon and Devika Subramanian*

AIC-96-013 Cognitive Modeling of Action Selection Learning, *Diana Gordon and Devika Subramanian*

AIC-96-014 Simplifying Decision Trees: A Survey, *Leonard A. Breslow and David W. Aha*

AIC-96-015 Comparing Tree-Simplification Procedures, *Leonard A. Breslow and David W. Aha*

AIC-96-016 A WWW Demonstration of Stratified Case-Based Reasoning, *Jefferey W. Adams and David W. Aha*

AIC-96-017 Model-based Pattern Recognition with Multilayer Neural Networks: Learning from the Eye, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-96-018 Proportional Selection and Sampling Algorithms, *John. J. Grefenstette*

AIC-96-019 Rank-based Selection, *J.ohn J. Grefenstette*

AIC-96-020 Efficient Implementations of Algorithms *J.ohn J. Grefenstette*

AIC-96-021 Methods for Competitive and Cooperative Co-evolution, *John J. Grefenstette and Robert Daley*

AIC-96-022 Genetic Learning for Adaption in Autonomous Robots, *John J. Grefenstette*

AIC-96-023 Situation Assessment Through Collaborative Human-Copmputer Interaction, *Scott D. Kushnier, Christof H. Heithecker, James A. Ballas, and Daniel C. McFarlane*

AIC-96-024 Cloud Classification Using Error-Correcting Output Codes, *David W. Aha and Richard L. Bankert*

AIC-96-025 Adjustable Graphic-Based Clustering Method, *Liwu W. Chang*

AIC-96-027 Multimodal Interaction With a Map-Based Simulation System, *Kenneth Wauchope*

AIC-96-028 A Proposal for Refining Case Libraries, *David W. Aha*

AIC-96-029 Developing Mult-layer Neural network for Environments of Interest to the Intelligence Community, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-96-030 RoboShepherd: Learning a Complex Behavior, *Alan C. Schultz, John J. Grefenstette and William Adams*

AIC-96-031 Robo-Shepherd: Learning Complex Robotic Behaviors, *Alan C. Schultz, John J. Grefenstette, and William Adams*

AIC-96-032 Shipboard VR: From Damage Control to Design, *Lawrence Rosenblum, Jim Durbin, Upul Obeysekare, Linda Sibert, David Tate, James Templeman, Joyti Agrawal, Daniel Fasulo, Thomas Meyer, Greg Newton, and Amit Shaley*

AIC-96-033 Individual Differences in World Processing Strategies, *J.G. Temple and Astrid Schmidt-Nielsen*

AIC-96-034 Speaker Recognizability Testing for Voice Coders, *Astrid Schmidt-Nielsen and Derek Brock*

AIC-96-035 Perceiving Talker Differences, *Astrid Schmidt-Nielsen*

AIC-96-036 Characterizing Human Ability To Discriminate Talkers Over Low Data Rate Voice Coders, *Astrid Schmidt-Nielsen*

AIC-96-037 Interfaces for Intelligent Control of Data Fusion Processing, James *A. Ballas, Daniel C. McFarlane, Lisa B. Achille, Janet L. Stroup, C.H.Heithecker, and S.D. Kushnier*

AIC-96-038 Computations Modeling of Multimodal I/O in Simulated Cockpits, *James A. Ballas*

AIC-96-039 Recombination Parameters, *William M. Spears*

AIC-96-040 Speciation Methods, *Kalyan Deb and William M. Spears*

AIC-96-041 Analyzing GAs Using Markov Models with Semantically Ordered and Lumped States, *William M. Spears and Kenneth A. De Jong*

AIC-96-042 Improvement To a Neural Network Cloud Classifier, *R.L. Bankert and David W. Aha*

AIC-96-043 Simulated Annealing for Hard Satisfiability Problems, *William M. Spears*

AIC-96-044 Workshop Report: Case-Based Reasoning, *David W. Aha*

1995 PUBLICATIONS

AIC-95-001 Stratified Case-Based Reasoning: Reusing Hierarchical Problem Solving Episodes, *L. Karl Branting and David W. Aha*

AIC-95-002 Extending the User Action Notation (UAN) for specifying Interfaces with Multiple Input Devices and Parallel Path Structure, *Lynn Dievendorf, Derek Brock, and Robert J.K. Jacob*

AIC-95-003 An Implementation and Experiment with the Nested Generalized Exemplars Algorithm, *David W. Aha*

AIC-95-004 For Every Generalization Action, Is There Really an Equal and Opposite Reaction? Analysis of the Conservation Law for Generalization Performance, *R. B. Rao, Diana F. Gordon, William M. Spears*

AIC-95-005 Unsupervised Classification Procedures Applied to Cloud Data, *Diana Gordon, Paul Tag, and Richard Bankert*

AIC-95-006 An Analysis of Communications and the Use of Military Terms in Navy Team Training, *Lisa B. Achille, Kay G. Schulze, and Astrid Schmidt-Nielsen*

AIC-95-007 Evaluation and Selection of Biases for Machine Learning, *Diana Gordon and Marie des Jardins*

AIC-95-008 Genetic Algorithms for Expert System Validation, *Edward A. Roache, Kenneth A. Hickok, Kenneth F. Loje, Michael W. Hunt, and John J. Grefenstette*

AIC-95-009 Automatic Target Extraction in Infrared Images, *Behrooz Kamgar-Parsi*

AIC-95-010 A Coevolutionary Approach to Learning Sequential Decision Rules, *Mitchell A. Potter, Kenneth A. De Jong, and John J. Grefenstette*

AIC-95-011 A Test of Speaker Recognition Using Human Listeners, *Astrid Schmidt-Nielsen*

AIC-95-012 Adaption of Knowledge for Reuse, *David Aha*, editor

AIC-95-013 Virtual Genetic Algorithms: First Results, *John Grefenstette*

AIC-95-014 Robot Learning with Parallel Genetic Algorithms on Networked Computers, *John Grefenstette*

AIC-95-015 Extending the User Action Notation for Research in Individual Differences, *Derek Brock, Lynn Dievendorf, Deborah Hix, and J. Greg Trafton*

AIC-95-016 Evolving Complex Structures via Cooperative Coevolution, *Kenneth A. De Jong and Mitchell A. Potter*

AIC-95-017 Evolving Neural Networks with Collaborative Species, *Mitchell A. Potter and Kenneth A. De Jong*

AIC-95-018 Mental Representations of Spatial Language, *Geoffrey S. Hubona, Stephanie S. Everett, Elaine Marsh, and Kenneth Wauchope*

AIC-95-019 A Paradigm to Assess and Evaluate Tools to Support the Software Development Process, *James. A. Ballas and Janet L. Stroup*

AIC-95-020 Interpreting the Language of Informational Sound, *James. A. Ballas*

AIC-95-021 Conversational Dialogue in Graphical User Interfaces: nteraction Technique Feedback and Dialogue Structure, *Manuel A. Pérez-Quiñones*

AIC-95-022 Applying Genetic Algorithms to the Testing of Intelligent Controllers, *Alan C. Schultz, John J. Grefenstette, and Kenneth A. De Jong*

AIC-95-023 Applying Machine Learning in Practice, *David Aha,* editor

AIC-95-024 A Testbed for Experiments in Adaptive Memory Retrieval and Indexing, *Li Wu Chang and Patrick Harrison*

AIC-95-025 Rejection of Unfamiliar Patterns with Multilayer Neural Networks, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-95-026 Weighting Features, *Dietrich Wettschereck and David W. Aha*

AIC-95-027 Learning to Break Things: Adaptive Testing of Intelligent Controllers, *Alan C. Schultz, John J. Grefenstette, and Kenneth A. De Jong*

AIC-95-028 Computational Pragmatics in HCI: Use of Dialog Context in a Multimodal Application, *Manuel A. Pérez-Quiñones*

AIC-95-030 VEG: Intelligent Workbench for Studying Earth's Vegetation, *Patrick R. Harrison, P. Ann Harrison, and Daniel S. Kimes*

AIC-95-031 Performance Evaluation of Navigation Algorithms Using Percolation Theory, *Ralph Hartley*

AIC-95-032 Advanced Interaction for Command and Control Planning Systems, *Linda E. Sibert and James N. Templeman*

AIC-95-033 A Methodology for Developing New Interaction Techniques, *Deborah Hix, James N. Templeman, Ankush Gosain, and Kapil Dandekar*

AIC-95-034 Pre-screen Projection: From Concept to Testing of a New Interaction Technique, *Deborah Hix, James N. Templeman, and Robert J.K. Jacob*

AIC-95-035 Virtual Environment Firefighting / Ship Familiarization Feasibility Tests Aboard the EX-USS *Shadwell, David Tate, Linda E. Sibert, F. W. Williams, LCDR Tony King, and Donald H. Hewitt*

AIC-95-036 Ecological Acoustics: Which Ecology? What Acoustics?, *James A. Ballas*

AIC-95-037 Navy Team Communications for Tactical Decision Making, *Lisa B. Achille, and Kay G. Schulze*

AIC-95-038 Distribution and Moments of the Weighted Sum of Uniform Random Variables with Applications in Reducing Monte Carlo Simulations, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh*

AIC-95-039 Rejection with Multilayer Neural Networks: Automatic Generation of the Training Set, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-95-040 Coding and Compression with Flexible Transforms, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Larry Schuette*

AIC-95-041 Why Do Now What Can Be Done Later?, *Scott Musman and Liwu Chang*

AIC-95-042 Knack: An Adaptive CBR Tool for Experimenting with Retrieval and Indexing, *Liwu Chang, Patrick R. Harrison, and Laura Davis*

AIC-95-043 Adapting Crossover in Evolutionary Algorithms, *William M. Spears*

AIC-95-044 Recombination Parameters, *William M. Spears*

AIC-95-045 Evolving Fuzzy Logic Control Strategies Using SAMUEL: An Initial Implementation, *Helen Cobb and John J. Grefenstette*

AIC-95-046 Toward Specification Techniques for Pre-Screen Projection and Other Next-Generation User Interfaces, *Robert J.K. Jacob and James Templeman*

AIC-95-047 Explicitly Biased Generalization, *Diana Gordon and D. Perlis*

AIC-95-048 A Wide-field Triangulation Laser Rangefinder for Machine Vision, *Frank Pipitone and Thomas Marshall*

AIC-95-049 A Hybrid Model Using Neural Networks and ACT–R, *J. Gregory Trafton*

AIC-95-051 Model-based Pattern Recognition with Multilayer Neural Networks: Learning From the Eye, *Behrooz Kamgar-Parsi and Behrad Kamgar-Parsi*

AIC-95-052 On Decentralizing Selection Algorithms, *Kenneth De Jong and Jayshree Sarma* code 5520

Communication Systems

The Communication Systems (CS) Branch is the principal agent for communication system design, analysis, and engineering, with current efforts focused on strategic, tactical and special warfare areas. Emphasis is given to network design, system performance validation via computer simulation experiments, modulation and coding techniques, communication terminal design and development, advanced instrumentation techniques, and equipment development. The Branch also provides consultation and support to other components of NRL, Navy, BMDO, and DoD in the areas of secure communication equipment, systems design and development, and warfare architecture.

Title: Lagrangian Techniques for Optimizing Throughput in Wireless Communication Networks Subject to QoS Constraints
Author(s): Gam D. Nguyen, Jeffrey E. Wieselthier, and Anthony Ephremides
E-mail Address: nguyen@itd.nrl.navy.mil or wieselthier@itd.nrl.navy.mil
Citation: Proceedings of the 31st Conference on Information Sciences and Systems (CISS). Baltimore, MD: The Johns Hopkins University, March 19-21, 1997, pp405-410
Date: March 19-21, 1997
Report No.: CS-97-001

Abstract

We study the problem of finding the input load that optimizes the total throughput in wireless communication networks, subject to the constraint that the blocking probability of each circuit stays below a threshold. Doing so permits us to "size" the capability of the network. Direct application of the traditional techniques of Lagrangian optimization to the problem often results in slow convergence to the optimal region because the optimizing trajectory progresses in a zigzag fashion in responding to the violation of the difficult constraints. To mitigate this undesirable behavior, we present a heuristic approach that attempts to guide the direction of the path leading to the optimal region. A projection vector is used in our algorithm to guide the search to proceed in a more direct path toward the optimal region.

Title: Ordinal Optimization of Discrete-Event Dynamic Systems: A Comparison of Standard Clock and Common-Random-Number Methods
Author(s): Jeffrey E. Wieselthier, Craig M. Barnhart, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: University of Maryland Conference on Information Sciences and Systems. Baltimore, MD: The Johns Hopkins University, March 19-21, 1997
Date: March 19-21, 1997
Report No.: CS-97-002

Abstract

In this paper we study the use of short simulation runs for ordinal optimization, where many experiments of structurally similar but parametrically different systems are stimulated in parallel. It is well known that the correlation introduced by the use of a common event sequence (such as that provided by Standard Clock (SC) simulation) facilitates the rapid determination of good policies. In this paper, we examine the question of whether the use of common random numbers (CRN), but different event sequences, to drive parallel experiments can provide similar rates of convergence. Although it has recently

been shown that CRN provides rapid convergence when certain conditions are satisfied, we have observed that the use of CRN provides little improvement over the use of independent similations for the admission-control problem studied in this paper.

Title: Design, Implementation, and Use of a Real-Time, Distributed Simulation Testbed for Mobile Communication Networks
Author(s): Dennis J. Baker
Citation: SPIE 11th Annual International Symposium on Aerospace/Defense Sensing, Simulation, and Controls. Orlando, FL, April 20-25, 1997
Date: April 20-25, 1997
Report No.: CS-97-003

Abstract

There is a need to design, develop, and test new mobile communication networks for military applications. The hardware cost to outfit a single node may be quite high. Much of the cost is in RF hardware, modems, and encryption devices. Replicating such costs over several nodes and adding the cost of maintaining a field site can quickly lead to unacceptable budget levels. One solution to this problem is, in the initial development and testing phase, to develop network communication systems that can operate with either real or simulated transmitters, receivers, modems, etc. This paper describes how we accomplished this task for the development of a High Frequency, Data/Voice (D/V) mobile network. The underlying, distributed, real-time simulation software evolved from Sun++. On top of this we built a simulation package to model mobile communication networks. Software for the Network Controller (NC) of the HF D/V Network was developed to work with these simulation packages as well as to work with real RF equipment. The NC software was tested in a 6-node network in which some of the RF equipment was simulated and some was real. The resultant system provides a testbed for examining the performance of command and control systems that must operate over mobile RF communication systems.

Title: Protocols to Support Integrated Services in a Mobile Cellular System Architecture
Author(s): James P. Hauser, Dale F. Lindquist, and R.K. Nair
E-mail Address: hauser@itd.nrl.navy.mil
Citation: 3rd International Command and Control Research and Technology Symposium. Washington, DC: National Defense University, June 17-20, 1997
Date: June 17-20, 1997
Report No.: CS-97-004

Abstract

Cellular systems are designed to provide a fixed amount of communication bandwidth to each mobile subscriber. Media access in digital systems is managed either by CDMA or a combination of DCMA and fixed TDMA. This works well when the system is servicing voice users that require uniform bandwidth reservations. However, this approach becomes inefficient when users are sending burst data traffic. Cellular providers are developing at least two sets of standards that address this issue - General Packet Radio Service (GPRS, European) and Cellular Digital Packet Data (CDPD, US). Our approach differs significantly from both of these emerging standards. We propose a single, integrated cellular system that accommodates both data (i.e., bursty, non-real-time datagram) and voice (i.e., real-time, virtual circuit) services with the ability to both reserve and dynamically reallocate bandwidth according to a user's current usage. We leverage previous work done at NRL in support of the Data and Voice Integration ATD. That work developed a unique cell multiplexing scheme that creates virtual channels for both datagram and virtual circuit services. We adapt this scheme to a cellular architecture by designing a new Medium Access Layer protocol for mobile subscriber transmissions.

Title: Hardware-In-The Loop Simulation and Prototyping with OPNET
Author(s): John S. Schlorff and Donald G. Kallgren
E-mail Address: schlorff@itd.nrl.navy.mil or kallgren@itd.nrl.navy.mil
Citation: OPNETWork '97 Conference Proceedings. Washington, DC, May 28-30, 1997
Date: May 28-30, 1997
Report No.: CS-97-005

Abstract

We modified OPNET models to interactively communicate in real-time with hardware devices over a LAN, allowing hardware in the loop simulations. The capabilities we added to our models enabled us to move from a simulation environment to a prototyping environment. We took an OPNET model of the Link-22 Naval communication system and partitioned it into independent component models, depicting discrete hardware components in the system. We added external asynchronous UDP/IP networking interfaces to the new models to allow them to communicate over a LAN, in real time, while running on separate computers. We synchronized the OPNET event queues with the host's system clock to within 10 to 50 milliseconds accuracy. This can only be done when a model's simulation time runs faster than or equal to real time.

Title: Classification of Error Locator Polynomials for Double Error Correcting BCH Codes
Author(s): Paul J. Crepeau
E-mail Address: crepeau@itd.nrl.navy.mil
Citation: Submitted to IEEE Transactions on Communications
Date 1997
Report No.: CS-97-006

Abstract

We give a complete classification of the error locator polynomials that occur in the decoding of DBC BCH codes. We present a new construction showing that all quadratic error locator polynomials produced by received vectors falling in the interstitial region between decoding spheres are illegitimate and have no roots. Futhermore, we show that a small subset of received vectors in the interstitial region produce cubic error locator polynomials that are illegitimate except for the correctable case of a triple error pattern with three equally spaced errors in the cyclic sense.

Title: A Polynomial Construction of Perfect Codes
Author(s): Gam D. Nguyen
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: Computers and Mathematics with Applications, v33, n8, April 1997, pp127-131
Date: April 1997
Report No.: CS-97-007

Abstract

Starting with a single-error-correcting extended perfect binary systematic code of length S, one can construct that of length S*(2**S) by polynomial manipulations.

Title: Summary and Applicability of Analog Fault Detection/Isolation Techniques
Author(s): J. A. Molnar
E-mail Address: molnar@itd.nrl.navy.mil
Citation: AUTOTESTCON '97, Anaheim, CA
Date: September 22-25, 1997
AIC Report No.: CS-97-008

Abstract

A survey of common analog fault diagnostic techniques is provided. The focus is on providing information to facilitate the use of viable techniques suited for a problem definition. The level of understanding of the analog system is correlated with the type of techniques best suited for the diagnostic system. Reviewed are techniques from Control Theory, Probability Theory,

Computational Expert Systems, and Computational Artificial Intelligence. The Control Theory techniques are suited best for system diagnostic problems where the system model is accurately understood. Techniques that employ Probability Theory are valuable for addressing uncertainty that arises in diagnostics of systems affected by noise. Computational Expert Systems address the problem of diagnostics by creating a data structure to represent the diagnostic process or system relationship representation. The technique can be used to great advantage in situations where the diagnostic process is accurately understood. Computational Artificial Intelligence techniques are presented as being best suited for systems where little reliable knowledge is known. The analysis does not preclude the use of any technique, but rather addresses efficiency of application.

Title: W-Band Synthesized Signal Generator using Fundamental Voltage Controlled Oscillators
Author(s): J. A. Molnar, R. Zborofsky
E-mail Address: molnar@itd.nrl.navy.mil
Citation: AUTOTESTCON '97, Anaheim, CA
Date: September 22-25, 1997
AIC Report No.: CS-97-009

Abstract

The architecture and implementation of a W-Band signal generator are described. The architecture presented highlights the developmental areas of the signal source, frequency control, output control and modulation. Voltage controlled oscillators (VCOs) were developed to provide frequency agility , to enhance the viability of frequency modulation (FM) characteristics, and to improve weight and power management requirements. Frequency control and phase coherence were achieved through the exploitation of digital phase lock loop (PLL) techniques. PIN diode attenuators that were developed cover the entire W-Band and provide the capacity for output level control. Additionally , the attenuators provide the capacity for amplitude modulation (AM) and pulse modulation (PM) because of the attenuation flatness (<5dB), large dynamic range (>40dB), and modulation bandwidth. A prototype has been developed to demonstrate the feasibility. The final implementation will be integrated into a C-sized VXI module chassis.

Title: Service Model and Cell Multiplexing for the Data and Voice Integration Advanced Technology Demostration

Author(s): James P. Hauser

E-mail Address: hauser@itd.nrl.navy.mil

Citation: MILCOM '97 Classified Conference Proceedings. Monterey, CA: IEEE, Nov. 2-5, 1997

Date: November 2-5, 1997

Report No.: CS-97-010

Abstract (Unclassified)

NRL's recently completed Data and Voice Integration Advanced Technology Demonstration successfully demonstrated integrated services using a mobile, 2.4 kbps, HF radio network. The methods successfully employed at this very low data rate are easily scaled to higher data rates. The service model includes both prioritized datagram services and virtual circuit services. Real-time applications, such as interactive voice, use the Resource Reservation Protocol (RSVP) API to request virtual circuit service via the Subnet Provider Interface (SNPI). The SNPI provides access to the radio network and the various services defined by the service model. These services are supported by cell multiplexing and adaptation layers that are similar to, yet distinct from those used by ATM switches.

Title: Algorithms for Finding Optimal Offered Load in Wireless Communication Networks

Author(s): Jeffrey E. Wieselthier, Gam D. Nguyen, and Anthony Ephremides

E-mail Address: wieselthier@itd.nrl.navy.mil or nguyen@itd.nrl.navy.mil

Citation: Proceedings of IEEE MILCOM '97. Monterey, CA, November 1997, Paper No. 41.06

Date: November 1997

Report No.: CS-97-011

Abstract

In this paper we study the problem of finding the input load that optimizes the total throughput in circuit-switched, multihop, wireless networks that are subject to QoS constraints on blocking probability. By doing so, we are able to "size" the network capability for a given admission-control policy, thereby determining how much traffic the network can support as well as the offered loads that achieve this optimum. A "projection algorithm," based on the use of Lagrangian optimization techniques and heuristics, is developed, and its behavior is investigated. Extensive computational results demonstrate that this algorithm provides reliable convergence to optimal solutions.

Title: Strategic Alliance for Advanced Navy COTS Test Equipment
Author(s): J. A. Molnar
E-mail Address: molnar@itd.nrl.navy.mil
Citation: Society of Logistics Engineers Technology Management Symposium & Expo, Hilton Head, SC
Date: November 17-19, 1997
AIC Report No.: CS-97-012

Abstract

The Navy under the direction of the Naval Sea Systems Command (NAVSEA) has, since 1973, implemented a policy of procuring almost exclusively Commercial-off-the-shelf (COTS) general purpose electronic test equipment (GPETE). This policy has been implemented through a number of methods to ensure that COTS GPETE meets the rigorous demands of deployment in military service. These methods are as follows: (a) a specification for general performance characteristics, MIL-PRF-28800F (formerly MIL-T-28800), (b) information sharing concerning prime system implementation of emerging technologies, (c) preview of new test equipment technology implementations, (d) advanced development and pre-production screening of new model features, and (e) maintenance of competitive pressures.

Title: Three Techniques for Ordinal Optimization: Short Simulation Runs, Crude Analytical Models, and Imprecise Simulation Models
Author(s): J.E. Wieselthier
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: Proceedings of the 1997 International Conference on Intelligent Systems and Semiotics: A Learning Perspective, (ISAS '97),.Gaithersburg, MD, Sept. 1997, pp175-180
Date: September 1997
Report No.: CS-97-013

Abstract

In the study of discrete-event dynamic systems (DEDS), accurate analytical models are generally either unavailable or too complex to evaluate numerically. Thus, the determination of optimal control policies often entails the simulation of many alternative systems in parallel. To reduce the computational burden, we investigate the use of ordinal optimization. This approach focuses on determining control policies that perform relatively well (although not necessarily optimally), without necessarily obtaining accurate performance measures.

In this paper we study three techniques for the ordinal optimization of DEDS, namely the use of short simulation runs, crude analytical models, and imprecise simulation models.

Title: STOW Network Technologies and Operational Lessons Learned
Author(s): Ray Cole, Barth Rose, Larry O'Ferrall, Julie Tarr, and LTC Paul Myers
E-mail Address: cole@itd.nrl.navy.mil
Citation: Simulation Interoperability Workshop. Orlando, FL: Simulation Interoperability Standards Organization
Date: 1997
Report No.: CS-97-014

Abstract

This paper examines the technologies developed and integrated to create the STOW Network and it discusses the operational lessons learned in running the largest ever trans-Atlantic, secure, distributed, entity level training simulation. Technical discussion will focus on the efficient and effective use of bandwidth for large scale exericises. The network features a highly dynamic IP multicast capable local area network, high speed ATM network using point-to-multipoint switched virtual circuits, virtual circuit management, and quality of service. The FASTLANE (KG-75) provided high speed network security. Operational considerations in managing a multi-site, international network operating in support of a classified training exercise will be discussed.

Title: A Recommended Error Control Architecture for ATM Networks with Wireless Links
Author(s): J.B. Cain and D.N. McGregor
E-mail Address: cain@itd.nrl.navy.mil or mcgregor@itd.nrl.navy.mil
Citation: IEEE Journal on Selected Areas on Communication, v15, n1, January 1997. pp16-28
Date: January 1997
Report No.: CS-97-015

This published article has no abstract.

Title: Performance and Resource Cost Comparisons for the CBT and PIM Multicast Routing Protocols
Author(s): T. Billhartz, J.B. Cain, E. Farrey-Goudreau, D. Fieg, and S.G. Batsell
E-mail Address: cain@itd.nrl.navy.mil
Citation: IEEE Journal on Selected Areas in Communication, v15, n3, April 1997, pp304-315
Date: April 1997
Report No.: CS-97-016

This published article has no abstract.

Tiitle: Naval Research Laboratory's Data/Voice ATD: HF Data/Voice Network
Author(s): D.J. Baker
E-mail Address: baker@itc.nrl.navy.mil
Citation: Presented at Mobile Ad Hoc Networking Workshop. College Park, MD: University of Maryland, March 14, 1997
Date: March 14, 1997
Report No.: CS-97-017

This paper has no abstract.

Title: Littoral Forces Communication
Author(s): D.N. McGregor
E-mail Address: mcgregor@itd.nrl.navy.mil
Citation: Presented at the DDR&E Information Systems & Technology Technology Assessment and Review, March 18, 1997
Date: March 18, 1997
Report No.: CS-97-018

This paper has no abstract.

Title: Networking Concepts Using SINCGARS SIP/INC Technology to Support Tactical Communications for Expeditionary Warfare Operations.
Author(s): D.N. McGregor and E.I. Althouse
E-mail Address: mcgregor@itd.nrl.navy.mil or althouse@its.nrl.navy.mil
Citation: Final Report, Naval Research Laboratory, Marris Corporation, ITT, Jan. 30, 1997
Date: January 30, 1997
Report No.: CS-97-019

This paper has no abstract.

Title: Use of SINCGARS in Littoral/Expeditionary Warfare
Author(s): J.B. Cain, et al.
E-mail Address: cain@itd.nrl.navy.mil
Citation: Final Report, Harris Corporation, Jan. 17, 1997
Date: January 17, 1997
Report No.: CS-97-020

This paper has no abstract.

Title: Joint Littoral Warfare Tactical Communications Requirements Analysis
Author(s): J. Lovuola
E-mail Address: lovuola@itd.nrl.navy.mil
Citation: Final Report, ITT, Jan. 31, 1997
Date: January 31, 1997
Report No.: CS-97-021

This paper has no abstract.

Title: Remote Digital Antenna Current Meter Modification
Author(s): T. H. Gattis
E-mail Address: gattis@itd.nrl.navy.mil
Citation: Internal Report
Date: August 1997
Report No: CS-97-022

Abstract

The Remote Digital Antenna Current Meter provides a means of measuring and displaying the antenna down lead current at the Navy's VLF/LF transmitter installations. These meters are used at sites where the antenna helix sites are separated from the transmitter building by distances from a few hundred feet to miles. When used in conjunction with a current transformer, the meter display will indicate the true rms value of the download current regardless of the type of modulation. The transmit unit measures the current signal level, converts the value to a digital word and outputs the signal in RS-232 format. The receiver unit receives the RS-232 digital signals, removes the current value word and displays the antenna down lead current. The current indicator is a four digit solid state display with a maximum value of 3999 amperes in the frequency range of 10 to 200 kilohertz (KHz).

1996 PUBLICATIONS

CS-96-001 A Simple Analysis of Average Queueing Delay in Tree Networks, *E. Modiano, J. E. Wieselthier, and A. Ephremides*

CS-96-002 Efficient Evaluation and Control of DEDS via Standard Clock Simulation and Ordinal Optimization Techniques, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-96-003 Performance and Resource Cost Comparisons for the CBT and PIM Multicast Routing Protocols in DIS Environments, *T. Billhartz, J. B. Cain, E. Farrey-Goudreau, D. Fieg, S. Batsell, and S. Milner*

CS-96-004 Constrained Optimization Methods for Admission Control and Offered Load in Communication Networks, *Craig M. Barnhart , Jeffrey E. Wiesethier, and Anthony Ephremides*

CS-96-005 Data Collection Using SNMP In the DIS Environment *D. N. McGregor, B. J. Root, and R. R. Nair*

CS-96-006 STOW Traffic and Related Issues, *G. D. Nguyen, and Stephen G. Batsell*

CS-96-007 A New Look At Double Error Correcting BCH Codes, *P. J. Crepeau,*

CS-96-008 Statistical Characteristics of DIS Traffic,*G. D. Nguyen and S. G. Batsell*

CS-96-009 New Reliable Error-Detection Codes and Their Fast Implementations, *G. D. Nguyen*

CS-96-010 Efficient Evaluation and Control of DEDS Via Standard Clock Simulation and Ordinal Optimization Techniques, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-96-011 A Fast Method for Combining/Generating Synthetic Traffic Traces Exhibiting Short- and Long-Range Dependence, *G. D. Nguyen*

CS-96-012 A Polynomial Construction of Perfect Codes, *G. D. Nguyen*

CS-96-013 Multiple-Ring Architecture and its FDDI Applications, *G. D. Nguyen*

CS-96-014 Conversion of MIL-T-28800 to a Performance Specification, *Joseph A. Molnar*

CS-96-015 A Problem of Constrained Optimization for Bandwidth Allocation in High-Speed and Wireless Communication Networks, *Jeffrey E. Wieselthier, Craig M. Barnhart, and Anthony Ephremides*

CS-96-016 A Recommended Error Control Architecture and Issues for ATM Networks with Wireless Links, *J. B. Cain, D. N. McGregor*

CS-96-017 Optimization of Admission Control in Wireless Networks, *J. E. Wieselthier, C. M. Barnhart, A. Ephremides*

CS-96-018 Mobile Internetworking Design Issues for Littoral and Expeditionary Warfare, *D. N. McGregor, E. L. Althouse, D. F. Gingras*

CS-96-019 An Error Control Architecture for ATM Networks with Wireless Links, *J. B. Cain, D. N. McGregor*

CS-96-020 Data/Voice Integration Advanced Technology Demonstration, *E. L. Althouse*

1995 PUBLICATIONS

CS-95-001 Admission-Control Policies for Multihop Wireless Networks, *Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides*

CS-95-002 Standard Clock Simulation and Ordinal Optimization Applied to Admission Control in Integrated Communication Networks, *J.E. Wieselthier, C.M. Barnhart and Anthony Ephremides*

CS-95-003 Multi-Access Strategies for an Integrated Voice/Data CDMA Packet Radio Network, *Mohsen Soroushnejad and Evaggelos Geraniotis*

CS-95-004 Ordinal Optimization of Admission Control in Wireless Multihop Integrated Networks via Standard Clock Simulation, *Jeffrey E. Wieselthier, Craig M. Barnhart, and A. Ephremides*

CS-95-005 Voice Management and Multiplexing Protocols Developed for the Data and Voice Integration Advanced Technology Demonstration, *James P. Hauser*

CS-95-006 Real-Time Network Packet Voice Support in the Data Voice Integration Advanced Technology Demonstration, *Joseph P. Macker*

CS-95-007 Quality Assurance, Alignment, and Test Procedure for the MD-1310/U Modulator, *J.A. Molnar and E.R. Farren*

CS-95-008 Novel Techniques for the Analysis of Wireless Integrated Voice/Data Networks, *Jeffrey E. Wieselthier, Craig M. Barnhart, and Anthony Ephremides*

CS-95-009 Integrated Computer Aided Design Practices as Demonstrated on A Fin-Line Device, *Joseph A. Molnar*

CS-95-010 MD-1310/U VLF/LF Modulator Functionality and Performance Test Report, *T.H. Gattis*

CS-95-011 Adding Training Capability to COTS Network Management Software, *Radhakrishnan R. Nair and Dennis N. McGregor*

CS-95-012 Tactical Radio Frequency Requirements for Next Generation Internet Protocols, *Robert B. Adamson*

CS-95-013 Coding and Synchronization Analysis of the NILE UHF Fixed-Frequency Waveform, *Paul J. Crepeau and John C. McCanless*

CS-95-014 On Burst-Error Detecting Capability of Weighted Sum Codes, *Gam D. Nguyen*

CS-95-016 IVOX The Interactive VOice eXchange Application, *Joseph P. Macker and R. Brian Adamson*

CS-95-017 A New Family of Reliable Error Detection Codes Having Low Complexity, *Gam D. Nguyen*

CS-95-018 A Neural Network Approach to Solving the Link Activation Problem in Multihop Radio Networks, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-95-019 Platform-Related Limitations to Efficiency in Standard Clock Simulation on Sequential Machines, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-95-021 Noise Issues in Optical Linear Algebra Processor Design, *S. G. Batsell, J. F. Walkup, and T. F. Krile*

CS-95-022 The Implications of a Distributed Computing Paradigm on Multicast Routing, *S. G. Batsell and J. E. Klinker*

CS-95-025 MCA Protocols and Algorithms, *K. Burrows, D. Nguyen, E. Rubin, E. Smythe, and W. Thoet*

CS-95-026 Performance Analysis of ATM Networks With Wireless Links, *J. B. Cain*

CS-95-027 Key Performance Issues for ATM Networks with Wireless Links, *J. B. Cain and D. N. McGregor*

CS-95-028 Parallel Sample Path Generation for Discrete Event Systems and the Traffic Smoothing Problem, *C. G. Cassandras and J. Pan*

CS-95-029 Scheduling Policies Using Marked/Phantom Slot Algorithms, *C. G. Cassandras and V. Julka*

CS-95-030 A Reservation Based Multicast (RBM) Routing Protocol for Mobile Networks: Initial Route Construction Phase, *M.S. Corson and S. G. Batsell*

CS-95-031 A Reservation Based Multicast (RBM) Routing Protocol for Model Networks: Initial Routing Construction, *M. S. Corson and S. G. Batsell*

CS-95-032 Admission Control and Bandwidth Allocation in High-Speed Networks as a System Theory Problem, *A. Ephremides, J. E. Wieselthier, and C. M. Barnhart*

CS-95-033 A Multiple-Access Scheme for Voice/Data Integration in Hybrid Satellite/Terrestrial Packet Radio Networks, *E. Geraniotis, M. Soroushnejad, and W. B. Yang*

CS-95-034 Adding SNMP Interface to Applications, *R. R. Nair*

CS-95-035 Design of SNMP Interface for Application Control Software, *R. R. Nair*

CS-95-036 Multi-Access Strategies for an Integrated Voice/Data CDMA Packet Radio Network, *M. Soroushnejad and E. Geraniotis*

CS-95-037 A Mini-Product-Form-Based Solution to Data-Delay Evaluation in Wireless Integrated Voice Data Networks, *J. E. Wieselthier, C. M. Barnhart, and A. Ephremides*

CS-95-038 Fixed- and Movable-Boundary Channel-Access Schemes for Integrated Voice/Data Networks, *J. E. Wieselthier and A. Ephremides*

CS-95-039 Data-Delay Evaluation in Integrated Wireless Networks based on Local Product-Form Solutions for Voice Occupancy, *J. E. Wieselthier, C. M. Barnhart, and A. Ephremides*

CS-95-040 Integrated Services in Tactical Communication Systems, *E. L. Althouse, J. P. Macker, J. P. Hauser, and D. J. Baker*

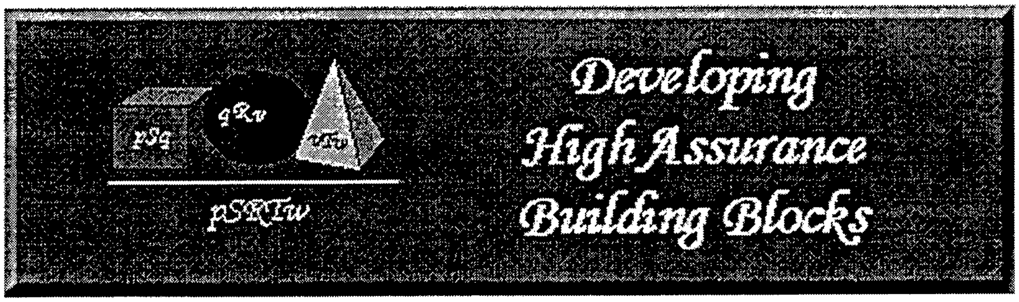
CS-95-041 Tri-Service Requirements and Growth Capabilities Report, *J. B. Cain and K. Kirk*

CS-95-042 Communication Systems Network Interoperability, *Robert B. Adamson*

code 5540

Center For High Assurance Computer Systems

The Center for High Assurance Computer Systems (CHACS) performs research and develops technology in areas supporting military requirements for communication security (COMSEC) and computer security (COMPUSEC). Emphasis is given to the development of concepts, architectures, analysis techniques and methodology that exploit appropriately the opportunities available through systematic consideration of the total security problem and its impact on communication and computer systems. The Center provides leadership and is the Navy's lead laboratory for research and development of COMPUSEC technology and evaluation techniques. Areas of activity include development of information security devices, subsystems and system technology through the conceptual, analysis and experimentation, and proof-of-concept phases. The Center works closely with Navy system developers and with the National Security Agency.



CENTER FOR HIGH ASSURANCE COMPUTER SYSTEMS

CODE 5540

Title: Human-Style Theorem Proving Using PVS
Author(s): Myla M. Archer and Constance L. Heitmeyer
E-mail Address: archer@itd.nrl.navy.mil or heitmeyer@itd.nrl.navy.mil
Citation: TPHOLs '97, Murray Hill, NJ
Date: August 19-22, 1997
Report No.: CHACS-97-001

Abstract

A major barrier to more common use of mechanical theorem provers in verifying software designs is the significant distance between proof styles natural to humans and proof styles supported by mechanical provers. To make mechanical provers useful to software designers with some mathematical sophistication but without expertise in mechanical provers, the distance between hand proofs and their mechanized versions must be reduced. To achieve this, we are developing a mechanical prover called TAME on top of PVS. TAME is designed to process proof steps that resemble in style and size the typical steps in hand proofs. TAME's support of more natural proof steps should not only facilitate mechanized checking of hand proofs, but in addition should provide assurance that theorems proved mechanically are true for the reasons expected and also provide a basis for conceptual level feedback when a mechanized proof fails. While infeasible for all applications, designing a prover that can process a set of high-level, natural proof steps for restricted domains should be achievable. In developing TAME, we have had moderate success in defining specialized proof strategies to validate hand proofs of properties of Lynch-Vaandrager timed automata. This paper reports on our successes, the services provided by PVS that support these successes, and some desired enhancements to PVS that would permit us to improve and extend TAME.

Title: Verifying SCR Requirements Specifications using State Exploration
Author(s): Ramesh Bharadwaj and Constance L. Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings of First ACM SIGPLAN Workshop on Automatic
Analysis of Software, Paris, France
Date: January 14, 1997.
Report No.: CHACS-97-003

Abstract

Researchers at the Naval Research Laboratory (NRL) have been developing a formal method, known as the SCR (Software Cost Reduction) method, to specify the requirements of software systems using tables. NRL has developed

a formal state machine model defining the SCR semantics and support tools for analysis and validation. Recently, a verification capability was added to the SCR toolset. Users can now invoke the Spin model checker within the toolset to establish properties of a specification. This paper describes the results of our initial experiments to verify properties of SCR requirements specifications using Spin. After reviewing the SCR requirements method and introducing our formal requirements model, we describe how SCR specifications can be translated into an imperative programming notation. We also describe how we limit state explosion by verifying abstractions of the original requirements specification. These abstractions are derived using the formula to be verified and special attributes of SCR specifications. The paper concludes with the results of our experiments with Spin and a discussion of ongoing and future work.

Title: Model Checking Complete Requirements Specifications Using Abstraction
Author(s): Ramesh Bharadwaj and Constance L. Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5540--97-7999
Date: November 10, 1997
Report No.: CHACS-97-005

Abstract

Although model checking has proven remarkably effective in detecting errors in hardware designs, its success in the analysis of software specifications has been quite limited. Model checking algorithms for hardware verification commonly use Binary Decision Diagrams (BDDs), a highly effective technique for analyzing specifications with the scores of Boolean variables commonly found in hardware descriptions. Unfortunately, BDDs are relatively ineffective for analyzing software specifications, which usually contain not only Booleans but variables spanning a wide range of data types. Further, software specifications have huge, often infinite, state spaces that cannot be model checked directly using conventional symbolic methods. One promising, but largely unexplored technique for limiting the size of the state space to be analyzed by model checking is to extract a model with a smaller state space from a complete specification using sound abstraction methods. Users of model checkers routinely analyze reduced models, but most often generate the models in ad hoc ways. As a result, the reduced models are often incorrect.

This report first describes how one can model check a complete requirements specification expressed in the SCR (Software Cost Reduction) tabular notation. Unlike previous approaches, which apply model checking to mode transition tables with Boolean variables, we use model checking to analyze properties of complete SCR specifications with variables ranging over many data types. The report also describes two sound and complete methods for producing abstractions from requirements specifications. These abstractions are derived from the specification based on the property to be analyzed. Finally, the report describes how SCR requirements specifications can be

translated into the languages of Spin, an explicit state model checker, and SMV, a symbolic model checker, and presents the results of model checking two sample SCR specifications using our abstraction methods and the two model checkers.

Title: Design and Assurance Strategy for the NRL Pump
Author(s): Myong H. Kang, Andrew P. Moore, and Ira S. Moskowitz
E-mail Address: kang@itd.nrl.navy.mil or moore@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: A brief version of this paper will appear in HASE97
Date: August 1997
Report No.: CHACS-97-007

Abstract

Developing a trustworthy system is difficult because the developer must construct a persuasive argument that the system conforms to its critical requirements. This assurance argument, as well as the software and hardware, must be evaluated by an independent certification team. In this paper, we present the external requirements and logical design of a specific trusted device, the NRL Pump, and describe our plan, called the assurance strategy, to create the eventual assurance argument. Our assurance strategy exploits currently available graphical specification, simulation, formal proof, and testing coverage analysis tools. Portions of the design are represented by figures generated by the Statemate toolset, and we discuss how those tools, and covert channel analysis, will be used to show that the logical design conforms to its external requirements. We conclude with some remarks on a possible physical architecture.

Title: The JMCIS Information Flow Improvement (JIFI) Assurance Strategy
Author(s): Andrew P. Moore
E-mail Address: moore@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5542--97-7951
Date: May 30, 1997
Report No.: CHACS-97-008

Abstract

The Joint Maritime Command Information System (JMCIS) provides a common operating environment for Naval tactical decision aids that currently operates two distinct system high enclaves, one at SECRET/GENSER and one at TOP SECRET/SCI. NRL Code 5540 is developing an extension of JMCIS, called JIFI (JMCIS Information Flow Improvement), to improve the timeliness and accuracy of GENSER information available to SCI JMCIS analysts while maintaining the security posture of the system. This document describes the strategy for developing the evidence that JIFI satisfies its critical security requirements. The strategy views databases in more classified enclaves as potential replica sites for data from less classified enclaves. Replicated data flows from lower enclaves to higher ones via simple one-way connections, yielding a high assurance MLS distributed system. The system high enclaves ensure discretionary security. The one-way connections are the only trusted component with respect to mandatory security. The JIFI architecture incorporates a one-way communications device, called the Pump, and existing COTS database replication technology to provide the extended JMCIS function. The JIFI assurance strategy described here complements and exploits modern system design methods, which separate data management from data processing, and enables effective low-cost MLS operation within that paradigm.

Title: Unlinkable Serial Transactions
Author(s): Paul F. Syverson, Stuart G. Stubblebine, and David M. Goldschlag
E-mail Address: syverson@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Financial Cryptography: First International Conference Proceedings (FC '97) v1318, pp39-55
Date: February 1997
Report No.: CHACS-97-009

Abstract

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. The protocol prevents the service from tracking the behavior of its customers while protecting the service vendor from abuse due to simultaneous or "cloned" usage from a single subscription. We present variants of the protocol supporting pay-per-use transactions within a subscription. We describe other applications including third-party subscription management, multivendor package sales, proof of group membership, and voter registration.

Title: Mobile Ad Hoc Networking (MANET): Routing Protocol Performance and Evaluation Considerations
Author(s): Joseph Macker and M. Scott Corson
E-mail Address: macker@itd.nrl.navy.mil
Citation: Internet Draft
Date: September 1997
Report No.: CHACS-97-010

Abstract

This memo describes the concept of mobile ad hoc networking--giving a rationale for its existence and outlining the unique issues and challenges. This document formulates a broad set of issues and presents a design framework for technology development with the IETF MANET Working Group.

Title: Reliable Multicast Transport and Integrated Erasure-Based Forward Error Correction
Author(s): Joseph Macker
E-mail Address: macker@itd.nrl.navy.mil
Citation: In Proceedings of IEEE MILCOM '97
Date: November 1997
Report No.: CHACS-97-011

Abstract

Multicast networking is an important emerging technology area for both commercial and military group-based data dissemination. In addition, a number of emerging applications can benefit from a reliable multicast transport service. A variety of approaches have been developed regarding the general application of Automatic Repeat Request (ARQ) techniques over Internet Protocol (IP) multicasting to achieve reliable delivery. In this paper, we investigate the application of erasure-based processing and parity-based recovery to a reliable multicast protocol framework. The integrated design approach described is shown to have improved efficiency and scalability features over reliable multicasting techniques based solely on ARQ. These bandwidth utilization improvements are expected to be substantial when applied across future multipoint communication infrastructures, especially over bandwidth-constrained and/or asymmetric networks.

Multicast networking is an important emerging technology area for both commercial and military group-based data dissemination. In addition, a number of emerging applications can benefit from a reliable multicast transport service. A variety of approaches have been developed regarding the general application of Automatic Repeat Request (ARQ) techniques over Internet Protocol (IP) multicasting to achieve reliable delivery. In this paper, we investigate the application of erasure-based processing and parity-based recovery to a reliable multicast protocol framework. The integrated design approach described is shown to have improved efficiency and scalability features over reliable multicasting techniques based solely on ARQ. These bandwidth utilization improvements are expected to be substantial when applied across future multipoint communication infrastructures, especially over bandwidth-constrained and/or asymmetric networks.

Title: Controlled Link Sharing and Reliable Multicast for Asymmetric Networks
Author(s): Joseph Macker and M. Scott Corson
E-mail Address: macker@itd.nrl.navy.mil
Citation: In Proceedings of Pacific Telecommunications Conference
Date: January 1997
Report No.: CHACS-97-012

Abstract

Satellites possess the ability to broadcast to an arbitrarily large, potentially mobile receiver population, and thus have a unique role to play in the future

Global Information Infrastructure (GII). To realize the seamless integration of satellites into the GII, one must consider not only the unique characteristics of satellite systems, but also the future composition of the GII. In this paper we will present a survey of the current and evolving Internet networking technologies and protocols that we think will, in the near term, constitute a major portion of the GII. We will put forth a taxonomy of issues that must be addressed to integrate asymmetric direct broadcast satellite (DBS) systems into the GII to support delivery of Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) Quality of Service (QoS)-based flows and reliable multicast data over asymmetric, high latency, limited bandwidth satellite links.

Title: Practical Defenses Against Storage Jamming
Author(s): J. McDermott and Judith N. Froscher
E-mail Address: mcdermott@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil
Citation: In Proceedings of the 20th National Information Systems Security Conference, Baltimore, MD, pp162-173
Date: October 1997
Report No.: CHACS-97-013

Abstract

Storage jamming is surreptitious tampering with stored data. The tampering can be done from within the application that manages the authentic storage, or it can be done from outside the application. Conventional security approaches such as access control, encryption, audit, and virus detection do not prevent storage jamming attacks. Attacks can be detected in real systems by replay or by replication.

Title: Rigorous Requirements for Real-Time Systems: Evolution and Application of the SCR Method
Author(s): Stuart Faulk and Constance Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, 3rd International Symposim on Requirements Engineering (RE '97)
Date: Jan. 6-10, 1997.
Report No.: CHACS-97-014

Abstract

This short paper describes a tutorial on the SCR (Software Cost Reduction) requirements method which was presented at RE '97.

Title: Verifying SCR Requirements Specifications Using State Exploration
Author(s): Ramesh Bharadwaj and Constance Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, First ACM SIGPLAN Workshop on Automated Analysis of Software
Date: January 14, 1997
Report No.: CHACS-97-015

Abstract

Researchers at the Naval Research Laboratory (NRL) have been developing a formal method, known as the SCR (Software Cost Reduction) method, to specify the requirements of software systems using tables. NRL has developed a formal state machine model defining the SCR semantics and support tools for analysis and validation. Recently, a verification capability was added to the SCR toolset. Users can now invoke the Spin model checker within the toolset to establish properties of a specification. This paper describes the results of our initial experiments to verify properties of SCR requirements specifications using Spin. After reviewing the SCR requirements method and introducing our formal requirements model, we describe how SCR specifications can be translated into an imperative programming notation. We also describe how we limit state explosion by verifying abstractions of the original requirements specification. These abstractions are derived using the formula to be verified and special attributes of SCR specifications. The paper concludes with the results of our experiments with Spin and a discussion of ongoing and future work.

Title: Verifying Hybrid Systems Modeled as Timed Automata: A Case Study, in Hybrid and Real-Time Systems
Author(s): Myla Archer and Constance Heitmeyer
E-mail Address: archer@itd.nrl.navy.mil or heitmeyer@itd.nrl.navy.mil
Citation: (HART'97), Lecture Notes in Computer Science, v1201. Springer-Verlag, pp.171-185
Date: 1997
Report No.: CHACS-97-016

Abstract

Verifying properties of hybrid systems can be highly complex. To reduce the effort required to produce a correct proof, the use of mechanical verification techniques is promising. Recently, we extended a mechanical verification system, originally developed to reason about deterministic real-time automata, to verify properties of hybrid systems. To evaluate our approach, we applied our extended proof system to a solution, based on the Lynch-Vaandrager timed automata model, of the Steam Boiler Controller problem, a hybrid systems benchmark. This paper reviews our mechanical verification system, which builds on SRI's Prototype Verification System (PVS), and describes the features we added to handle hybrid systems. It also discusses some errors we detected in applying our system to the benchmark problem. We conclude with a

summary of insights we acquired in using our system to specify and verify hybrid systems.

Title: Formal Methods for Real-Time Computing: A Panacea or Academic Poppycock
Author(s): Constance Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, Z Users' Meeting (ZUM '97), Lecture Notes in Computer Science, v1212, Springer-Verlag (Keynote Talk)
Date: 1997
Report No.: CHACS-97-017

Abstract

Much has been written in the past decade about the usefulness of formal methods for developing computer systems. In this talk, I describe first what I mean by a formal method, discuss some systems to which formal methods have been successfully applied recently, and present several guidelines that I and my colleagues have found useful in applying formal methods in the development of practical systems and software. I conclude with a summary of what has been accomplished to date and why some skepticism about the utility of formal methods in computer system development remains well-founded.

Title: Rigorous Requirements for Real-Time Systems: Evolution and Application of the SCR Method
Author(s): Stuart Faulk and Constance Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, International Conference on Software Engineering
Date: May 17-23, 1997
Report No.: CHACS-97-018

Abstract

This half-day tutorial provides an in-depth introduction to the SCR (Software Cost Reduction) requirements method, a practical, industrial-strength approach to formal requirements specification. Topics covered in the tutorial include the industrial perspective on formal methods, necessary attributes of methods and tools appropriate for industrial development of requirements, how the SCR method addresses common industrial concerns, the SCR requirements model, the SCR, toolset, technology transfer efforts, and results and lessons learned from application of the SCR method to a commercial software development effort.

Title: The SCR Method for Specifying, Verifying and Validating Requirements
Author(s): Constance Heitmeyer, James Kirby, and Bruce Labaw
E-mail Address: heitmeyer@itd.nrl.navy.mil or kirby@itd.nrl.navy.mil or labaw@itd.nrl.navy.mil
Citation: Proceedings, International Conference on Software Engineering
Date: May 17-23, 1997
Report No.: CHACS-97-019

Abstract

SCR*, a set of tools for developing and analyzing requirements specifications for real-time embedded systems, is described. The tools, based on a formal requirements model, include a specification editor, a consistency checker, a simulator, and a verifier.

Title: Tools for Formal Specification, Verification and Validation of Requirements
Author(s): Constance Heitmeyer, James Kirby, and Bruce Labaw
E-mail Address: heitmeyer@itd.nrl.navy.mil or kirby@itd.nrl.navy.mil or labaw@itd.nrl.navy.mil
Citation: Proceedings of 12th Annual Conference on Computer Assurance (COMPASS '97), Gaithersburg, MD
Date: June 16-19, 1997
Report No.: CHACS-97-020

Abstract

Although formal methods for developing computer systems have been available for more than a decade, few have had significant impact in practice. A major barrier to their use is that software developers find formal methods difficult to understand and apply. One exception is a formal method called SCR for specifying computer system requirements which, due to its easy to use tabular notation and its demonstrated scalability, has already achieved some success in industry. Recently, a set of software tools, including a specification editor, a consistency checker, a simulator, and a verifier, has been developed to support the SCR method \cite {COMPASS,tosem,aas}. This paper describes recent enhancements to the SCR tools: a new dependency graph browser which displays the dependencies among the variables in the specification, an improved consistency checker which produces detailed feedback about detected errors, and an assertion checker which checks application properties during simulation. To illustrate the tool enhancements, a simple automobile cruise control system is presented and analyzed.

Title: A Flexible, Extensible Simulation Environment for Testing Real-Time Specifications
Author(s): Brockmeyer, Monica, Farnam Jahanian, Constance Heitmeyer, and Bruce Labaw
E-mail Address: heitmeyer@itd.nrl.navy.mil or labaw@itd.nrl.navy.mil
Citation: Proceedings, Real-Time Applications Symposium (RTAS '97)
Date: June, 1997
Report No.: CHACS-97-021

Abstract

This paper describes MTSim, an extensible, customizable simulation platform for the Modechart toolset (MT). MTSim provides support for ``plugging in" user-defined viewers useful in simulating system behavior in different ways, including application-specific ways. MTSim also supports full user participation in the generation of simulations by allowing users to inject events into the execution trace. Moreover, MTSim provides monitoring and assertion checking of execution traces and the invocation of user-specified handlers upon assertion violation. This paper also introduces a MTSim component called WebSim, a suite of simulation tools for MT, and an an application-specific component of MTSim, which displays the cockpit of an F-18 aircraft and models its bomb release function.

Title: Applying the SCR Requirements Method to a Simple Autopilot
Author(s): Ramesh Bharadwaj and Constance Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, Fourth NASA-Langley Formal Methods Workshop (Lfm97), Hampton, VA
Date: September 10-12, 1997
Report No.: CHACS-97-022

Abstract

Although formal methods for developing computer systems have been available for more than a decade, few have had significant impact in practice. A major barrier to their use is that developers find formal methods difficult to understand and apply. One exception is a formal method called SCR for specifying computer system requirements which, due to its easy-to-use tabular notation and demonstrated scalability, has achieved some success in industry.

To demonstrate and evaluate the SCR method and tools, we recently used SCR to specify the requirements of a simplified mode control panel for the Boeing 737 autopilot. This paper presents the SCR requirements specification of the autopilot, outlines the process we used to create the SCR specification from a prose description, and discusses the problems and questions that arose in developing the specification. Formalizing and analyzing the requirements specification in SCR uncovered a number of problems with the original prose description, such as incorrect assumptions about the environment, incompleteness, and inconsistency. The paper also introduces a new tabular format we found useful in understanding and analyzing the required behavior of the autopilot. Finally, the paper compares the SCR approach to requirements with that of Butler, who uses the PVS language and prover to represent and analyze the autopilot requirements.

Title: Replication Does Survive Information Warfare Attacks
Author(s): John McDermott
E-mail Address: mcdermott@itd.nrl.navy.mil
Citation: Proceedings of the 11th Annual Working Conference on Database Security, Lake Tahoe, CA, pp186-198
Date: August 1997
Report No.: CHACS-97-024

Abstract

Recent literature on information warfare has suggested that general replication is not useful in dealing with storage spoofing attacks. We show that special cases of replication are useful not only in detecting but also in recovering from storage spoofing attacks.

Title: Doc, Wyatt, and Virgil: Prototyping Storage Jamming Defenses
Author(s): J. McDermott, R. Gelinas, and S. Orenstein
E-mail Address: mcdermott@aic.nrl.navy.mil
Citation: Proceedings of the 13th Annual Computer Security Applications Conference, San Diego, CA, pp. 265-273
Date: December 1997
Report No.: CHACS-97-025

Abstract

This paper describes progress to date on three prototype tools for detecting storage jamming attacks. One prototype uses a replay defense; another uses logical replication, and the third can be used to determine the source and pattern of a detected attack. Three prototype jammers are used to test the effectiveness of the defenses. Initial experiments have shown that access control, encryption, audit, and virus detection do not prevent or detect storage jamming. The prototype tools have been effective in detecting the same attacks. Object-oriented data storage may require the use of application-specific techniques for applying checksums.

Title: OR/SM: A Prototype Integrate Modeling Environment Based on Structured Modeling
Author(s): G. P. Wright, N. D. Worobetz, M. H. Kang, R. V. Mookerjee, and R. Chandrasekharan
E-mail Address: kang@itd.nrl.navy.mil
Citation: INFORMS Journal of Computing, v9, n2, Spring 1997, pp134-153
Date: 1997
Report No.: CHACS-97-026

Abstract

This article describes the design and implementation of (OR/SM), a computerized modeling environment based on Structured Modeling. The uniqueness of OR/SM is in the following: (1) the use of ORACLE Tools and Database as the delivery platform; (2) automatic and interactive links to SAS, a powerful and widely used commercial statistical analysis software system and optimization solver; and (3) an interactive link to QS(Quantitative Systems)-a commercial software package for solving wide range of operations management models. Some other key features are: (1) automatic generation of relational database tables for model data; (2) interactive checking of model syntax and semantics; and (3) automatic generation of several reference documents. Examples from blending, inventory control, and marketing mix management are used to illustrate the capabilities of OR/SM.

Title: Reducing Uncertainty About Common-Mode Failures
Author(s): J. Voas, J., A. Ghosh, L. Kassab, and F. Charron
Citation: Proceedings of International Symposium on Software Reliability Engineering
Date: November 1997
Report No.: CHACS-97-027

Abstract

Multi-version programming is employed in fault-tolerant computer systems in order to provide protection against common-mode failure in software. Multi-version programming involves building diverse software implementations of critical functions. The premise of building diverse versions is that the likelihood of a programming error in one version causing a failure in an identical manner as an error in another version is reduced. Skeptics of multi-version programming have correctly pointed out that common-mode failures between redundant diverse versions can reduce the return on investment in creating diverse versions.

To date, other than using historical data from other projects, there has been no way to estimate the potential for a given multi-version programming system to suffer a common-mode failure. This paper presents an algorithm and software analysis prototype to reduce the uncertainty of whether software flaws in diverse versions can result in common-mode failure. The analysis uses software fault-injection techniques to subject one or more versions to anomalous behavior. From this, we can predict how the software will behave if real faults exist in the multiple versions.

Title: Simulating Specification Errors and Ambiguities in Systems Employing Diversity
Author(s): J. Voas and L. Kassab
Citation: Proceedings of Pacific Northwest Software Quality Conference
Date: October 1997
Report No.: CHACS-97-028

Abstract

This paper looks at methods for predicting how likely it is that an n-version software system will suffer from common-mode failures. Common-mode failures are frequently caused by specification errors, specification ambiguities, and programmer faults. Since common-mode failures are detrimental to n-version systems, we have developed a method and a tool that observes the impact of simulated specification errors and specification ambiguities. These observations are made possible by a new family of fault injection algorithms designed to simulate specification anomalies. As a side-benefit, this analysis also provides clues concerning which portions of the specification, if even slightly wrong or misinterpreted, will lead to identical failures by two or more versions. This suggests which specification directives have the most impact on the system's functionality.

Title: Protocols using Anonymous Connections: Mobile Applications
Author(s): M. G. Reed, Paul Syverson, and David M. Goldschlag
E-mail Address: reed@itd.nrl.navy.mil or syverson@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the 5th International Workshop, Paris, France, Springer Verlag, v1361, pp13-23
Date: April 1997
Report No.: CHACS-97-029

Abstract

This paper describes security protocols that use anonymous channels, which do not reveal their endpoints, as primitive, much in the way that key distribution protocols take encryption as primitive. This abstraction allows us to focus on high level security goals of these protocols much as abstracting away from encryption clarifies and emphasizes high level security goals of key distribution protocols. The protocols described are for mobile applications that protect the location information of the participating principals.

Title: An Insecurity Model
Author(s): I.S. Moskowitz and M. H. Kang
E-mail Address: moskowitz@itd.nrl.navy.mil or kang@itd.nrl.navy.mil
Citation: New Security Paradigms Workshop
Date: 1997
Report No.: CHACS-97-030

Abstract

We examine a new way of looking at security violations, called insecurity flow. We express our new paradigm via a formal mathematical model that combines elements of graph theory and discrete probability. Prior work by Moore and Shannon on building reliable circuits out of unreliable components, and the physics community's interest in dynamical systems, especially percolation theory, motivates our work.

Title: Protecting Unattended Computers Without Software
Author(s): Carl E. Landwehr
E-mail Address: landwehr@itd.nrl.navy.mil
Citation: Thirteenth Annual Computer Security Applications Conference, San Diego, CA, pp274-283
Date: December 1997
Report No.: CHACS-97-031

Abstract

In many environments, users login to workstations and then leave them unattended. Rather than trying to stop users from doing what comes naturally, this paper suggests a simple, hardware-based system that can protect computers in such an environment from unauthorized use by those with physical access to the monitor and keyboard. Requirements for the system are described, some design issues are discussed, and a sketch of a design for an initial prototype is provided, together with an assurance argument for it. A prototype implementing many of the concepts described has been built; two dozen copies of a second prototype are soon to be installed in an office environment.

Title: Security Issues in Networks with Internet Access
Author(s): C.E. Landwehr and David M. Goldschlag
E-mail Address: landwehr@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: IEEE Proceedings, v85, n12, pp2034-2051
Date: December 1997
Report No.: CHACS-97-032

Abstract

This paper describes the basic principles of designing and administering a relatively secure network. The principles are illustrated by describing the

security issues a hypothetical company faces as the networks that support its operations evolve from strictly private, through a mix of Internet and private nets, to a final state in which the Internet is fully integrated into its operations, and the company participates in international electronic commerce. At each stage, the vulnerabilities and threats that the company faces, the countermeasures that it considers, and the residual risk the company accepts are noted. The paper concludes with a discussion of security policies and building blocks for secure networks.

Title: Safe Use of the Internet for Defence Purposes. TTCP STP-11 Report
Author(s): Carl E. Landwehr, et. al.
E-mail Address: landwehr@itd.nrl.navy.mil
Citation: TTCP Document, DOC-C3I-1, 1997
Date: May 1997
Report No.: CHACS-97-033

Abstract

This report, developed by the members of TTCP STP-11 in the spring of 1997, documents why Defence establishments of the TTCP member nations are increasing their use of the Internet and suggests guidelines for using the Internet safely and prudently for Defence purposes. It describes Internet architecture and vulnerabilities, current and emerging technologies that can be used to reduce the risks, and possible demonstrations of existing and emerging technologies.

Title: Private Web Browsing
Author: Paul F. Syverson, Michael G. Reed, and David M. Goldschlag
E-mail Address: syverson@itd.nrl.navy.mil or reed@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Journal of Computer Security, Special Issue on Web Security, v5, n3, pp237-248
Date: 1997
Report No.: CHACS-97-034

Abstract

This paper describes a communications primitive, anonymous connections, that support bidirectional and near real-time channels that are resistant to both eavesdropping and traffic analysis. The connections are made anonymous, although communication need not be. These anonymous connections are versatile and support private use of many different Internet services. For our purposes, privacy means maintaining the confidentiality of both the data stream and the identity of communicating parties. These are both kept confidential from network elements as well as external observers. Private Web browsing is achieved by unmodified Web browsers using anonymous connections by means of HTTP proxies. Private Web browsing may be made anonymous too

by a specialized proxy that removes identifying information from the HTTP data stream. This article specifies anonymous connections, describes our implementation, and discusses its application to Web browsing via HTTP proxies.

Title: Privacy on the Internet
Author(s): David M. Goldschlag, Michael G. Reed, and Paul F. Syverson
E-mail Address: goldschlag@itd.nrl.navy.mil or reed@itd.nrl.navy.mil or syversson@itd.nrl.navy.mil
Citation: INET '97, Kuala Lumpur, Malaysia
Date: June 1997
Report No.: CHACS-97-035

Abstract

The World Wide Web is rapidly becoming an important tool for modern day communication and commerce. But electronic messages sent over the Internet can be easily snooped and tracked revealing who is talking to whom and what they are talking about. Is privacy important and how can it be guaranteed? This paper describes how a freely available system, onion routing, can be used to provide privacy for a wide variety of Internet services, including Virtual Private Networks, Web browsing,e-mail, remote login, and electronic cash.

Title: Internet Communication Resistant to Traffic Analysis
Author(s): David M. Goldschlag, Michael G. Reed, and Paul F. Syverson
E-mail Address: goldschlag@itd.nrl.navy.mil or reed@itd.nrl.navy.mil or syverson@itd.nrl.navy.mil
Citation: 1997 NRL Review, Naval Research Laboratory Publication, NRL/PU/5230--97-320, pp109-111
Date: April 1997
Report No.: CHACS-97-036

Abstract

Determining who is talking to whom (called traffic analysis) is an important source of intelligence information. As military grade communication devices increasingly depend on the public communications infrastructure, it is important to use that infrastructure in ways that are resistant to traffic analysis. It may also be useful to communicate anonymously, for example when gathering intelligence from public databases. We describe bidirectional and real-time Anonymous Connections that are strongly resistant to eavesdropping and traffic analysis attacks by both insiders and outsiders. If necessary, communication is made anonymous by removing identifying information from the data stream. These anonymous connections have been prototyped in a system that protects the privacy of communication over the Internet and, in particular, the World Wide Web. Anonymous connections can protect both identity and location in many switched communication systems, such as wired, cellular, or satellite phone networks.

Title: Anonymous Connections and Onion Routing
Author(s): Michael G. Reed, Paul F. Syverson, and David M. Goldschlag
E-mail Address: reed@itd.nrl.navy.mil or syverson@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: IEEE Symposium on Security & Privacy, Oakland, CA, May 1997
Date: May 1997
Report No.: CHACS-97-037

Abstract

Onion Routing provides *anonymous connections* that are strongly resistant to both eavesdropping and traffic analysis. Onion routing accomplished this goal by separating identification from routing. Connections are always anonymous although commincation need not be. Unmodified Internet applications may use these anonymous connections by means of proxies. The proxies may also make communication anonymous by removing identifying information from the data stream. Onion routing has been implemented on Sun Solaris 2.x with proxies for Web browsing, remote logins, and e-mail. This paper discribes onion routing, our threat model, and the system's vulnerabilities.

Title: A Client-Seriver Architecture Supporting MLS Interoperability with COTS Components
Author(s): J.N. Froscher and M.H. Kang
E-mail Address: froscher@itd.nrl.navy.mil or kang@itd.nrl.navy.mil
Citation: Proceedings, MILCOM 97, Monterey, CA
Date: November 1997
Report No.: CHACS-97-038

Abstract

A major challenge facing the MLS community is to find ways to provide the information and connectivity that DoD users demand without either imposing unacceptable security risks or requiring expensive hardware and software that fails to mesh with commercial off-the-shelf (COTS) applications. This paper proposes, very briefly, an architecture that meets these goals using only a small number of relatively simple, low cost, high assurance components in combination with a preponderance of unmodified COTS hardware, operating systems and applications.

Title: Design and Assurance Strategy for the NRL Pump
Author(s): M.H. Kang, J.N. Froscher, and I.S. Moskowitz
E-mail Address: kang@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: 2nd IEEE High Assurance System Engineering Workshop
Date: 1997
Report No.: CHACS-97-039

Abstract

Developing a trustworthy system is difficult because the developer must construct a persuasive argument that the system conforms to its critical requirements. This assurance argument, as well as the software and hardware, must be evaluated by an independent certification team. In this paper, we present the external requirements and logical design of a specific trusted device, the NRL Pump and describe our plan, called the assurance strategy, to create the eventual assurance argument. Our assurance strategy exploits currently available graphical tools. Portions of the design are represented by figures generated by the Statemate toolset, and we discuss how those tools, and covert channel analysis, will be used to show that the logical design conforms to its external requirements. We conclude with some remarks on a possible physical architecture.

Title: A Different Look at Secure Distributed Computation
Author(s): Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: Proceedings of the 10th IEEE Computer Security Foundations Workshop (CSFW10), IEEE CS Press, pp109--115
Date: June 1997
Report No.: CHACS-97-040

Abstract

We discuss various aspects of secure distributed computation and look at weakening both the goals of such computation and the assumed capabilities of adversaries. We present a new protocol for a conditional form of probabilistic coordination and present a model of secure distributed computation in which friendly and hostile nodes are represented in competing interwoven networks of nodes. It is suggested that reasoning about goals, risks, tradeoffs, etc. for this model be done in a game-theoretic framework.

Title: On Searching for Known and Chosen Cipher Pairs Using the NRL Protocol Analyzer
Author(s): Stuart G. Stubblebine and Catherine A. Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of the DIMACS Workshop on Design and Formal Verification of Security Protocols
Date: September 1997
Report No.: CHACS-97-041

Abstract

Formal methods have been successfully applied to exceedingly abstract system specifications to verify high level security properties such as authentication, key exchange, and fail-safe revocation. Furthermore, considerable research exists on evaluating particular ciphers and secure hash functions used to implement high level security properties. However, verifying that less abstract system specifications satisfy low level security properties has been largely impractical. This is evidenced by innumerable system vulnerabilities where high level properties are not attained due to failed assumptions of low level properties. This paper presents ongoing work on investigating known and chosen ciphertext pairs using the NRL Protocol Analyzer. We describe a formal model of known and chosen pairs, and map it to the NRL Protocol Analyzer model. We also describe the use of the Analyzer to rediscover attacks on an early version of the ESP protocol, and show how our experience in using it has led us to refine our model. This was the first use of the Analyzer to model protocols at such a low level of abstraction.

Title: Detecting Attacks on Mobile Agents
Author(s): Catherine A. Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of the DARPA Foundations for Secure Mobile Code Workshop
Date: March 1997
Report No.: CHACS-97-042

Abstract

In this paper we consider the problem of determining whether or not data that has been gathered by an agent visiting multiple sites has been tampered with. We show how ``detection objects," a technique currently under investigation at NRL as a means of detecting malicious modification of databases, can be used to solve this problem.

Title: Three Paradigms in Computer Security
Author(s): Catherine A. Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of the 1997 New Security Paradigms Worskhop
Date: September, 1997
Report No.: CHACS-97-043

Abstract

This paper describes three paradigms in computer security in terms of how they relate to the existing infrastructure : by existing within it, replacing it, or by extending it or replacing only small portions. We identify the third as the most desirable, and discuss some of the implications of this approach.

Title: Critical Analysis of Security in Voice Hiding Techniques
Author(s): L. Chang and I. Moskowitz
E-mail Address: chang@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: Proceedings of International Conference of Information and Communication Security, Springer-Verlag, pp203-216
Date: November 11-14, 1997
Report No.: CHACS-97-044

Abstract

This paper provides a comparative assessment of detection in certain voice hiding techniques. The assessment is based on the complexity of breaking the stego key, the robustness of the hiding techniques, and the stego transmission rate. Unlike cryptography, to break the stego key in voice communication requires not only an extensive search but also estimation techniques for determining the values of parameters used in data embedding. We also consider disturbing embedded data in case resource constraints are imposed.

Title: An Architecture for Multilevel Secure Interoperability
Author(s): M.H. Kang, J.N. Froscher, and I.S. Moskowitz
E-mail Address: kang@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: Proceedings of the 13th Annual Computer Security Applications Conference, pp194-204
Date: 1997
Report No.: CHACS-97-045

Abstract

As computer systems become distributed and heterogeneous, there is strong movement in the commercial sector to ease the problems of interoperability and security. Many standards have been proposed for these problems. However, the commercial sector has not shown strong interest in providing cost-effective high-assurance multilevel security (MLS) solutions to the relatively small communities (e.g., intelligence, military) that require them. In this paper, we introduce a practical, cost-effective, and high-assurance secure solution for multilevel distributed and heterogeneous environments using COTS components. The solution is based on an MLS architecture that consists of commercial single-level hardware and software, and a few specialized security devices. We show how an MLS CORBA can be constructed from single-level CORBAs and two security devices; the NRL Pump and the Starlight Interactive Link. We also introduce the concept of MLS cooperative computing which is a way to semi-automate distributed computing among organizations at different security levels.

Title: Protection (Security) Models and Policy
Author(s): C.E. Landwehr
E-mail Address: landwehr@aic.nrl.navy.mil
Citation: The Computer Science and Engineering Handbook, CRC Press/Association for Computing Machinery, pp 1914-1924
Date: 1997
Report No.: CHACS-97-046

This report has no abstract.

Title: Computer Security, the Good, the Bad, and the Ugly,
Author(s): Catherine Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of the High Assurance Systems Engineering Workshop IEEE Computer Society Press, pp. 52-54
Date: 1997
Report No.: CHACS-97-047

Abstract

In this paper we discuss and characterize different types of solutions to computer security problems in terms of bad (theoretically sound, but expensive and impractical), ugly (practical, but messy and of doubtful assurance), and good (theoretically sound and practical). We also attempt to characterize the different approaches and problems in computer security that would lead to these different types of solutions.

Title: Panel: What Protocol Designers Need From Formal Methods
Author(s): Catherine Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of DIMACS Workshop on Design and Formal Verification of Security Protocols
Date: September, 1997
Report No.: CHACS-97-048

Abstract

The past few years have seen a rapidly growing amount of research in the application of formal methods to the design and verification of cryptographic protocols. They have also seen an equally rapidly growing amount of work in developing and fielding cryptographic protocols, and a growing need for secure communication over the Internet. The problem of assuring the correctness of these protocols has been a matter of some concern, and this sparked interest in making use of the products of formal methods research. However, formal methods has traditionally been seen as an arcane field requiring special expertise, and for this reason difficult to transition into industry.

The purpose of a this panel is to examine the issues around the question of making formal methods for cryptographic protocol analysis into tools that can be used by developers. We have invited a panel of experts on cryptographic protocol development to talk about what they need and expect from formal methods tools and techniques, and in what direction they would like the field to be going.

Title: Panel on Languages for Formal Specification of Security Protocols
Author(s): Catherine Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: 10th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press
Date: June 1997
Report No.: CHACS-97-049

Abstract:

In the last year or so, research in the formal analysis of cryptographic protocols has matured to the point where researchers are going beyond the mechanics of verification and considering the problem of providing specification languages that make it easier to specify protocols for analysis. A number of different approaches are being applied. Some are modifying existing formal specification languages, while others are implementing languages that are closely based on existing informal specification styles. Likewise, some are implementing languages that are closely tied to existing tools, while others are implementing tool-independent languages. An effort is also underway to develop a common language, CAPSL, that will serve as an interface to other tools and languages.

The purpose of this panel is to bring together those who are working on this problem and have us compare notes and explore current issues.

Title: Reducing the Risk of Multi-Level Secure (MLS) Workstations
Author(s): J. Eric Klinker and David M. Mihelcic
E-mail Address: library@aic.nrl.navy.mil
Citation: IEEE Milcom 1997, Monterey, CA, Nov. 2-5, 1997
Date: Nov. 2-5, 1997
Report No.: CHACS-97-050

Abstract

Great interest exists within the military in using recent advances in Multi-Level Secure (MLS) technology to improve operational capability. However, many practical operational applications demand more from the technology from an assurance standpoint than is currently available in most commercial MLS products. For example, following a strict "Yellow book" [3] definition for the separation of DoD Secret to Unclassified requires B3 level technology.

The most usable commercial MLS products on the market today are targeted at the B1 level, a substantial reduction in assurance from the B3 mandated by the Yellow Book. However the "Yellow Book" was merely written as a guideline for applying MLS technology. While there is certainly some risk associated with using B1 level technology, there are practical measures that can be taken to substantially reduce the risk of using B1 level technology.

This paper documents several techniques we have employed on several MLS installations in the Navy. The techniques are designed to reduce the overall risk of penetration on the systems. While many of the techniques can be used to improve the security of most Unix operating systems, they particularly reduce the operational risk of using an MLS operating system.

Title: A Thread-Local Storage Class for Win32
Author(s): Bruce Montrose
E-mail Address: montrose@itd.nrl.navy.mil
Citation: C++ Users Journal, Nov. 1997, v15, n11, pp49(4)
Date: Nov. 1997
Report No.: CHACS-97-051

Abstract

In many cases programmers working on multithreaded applications will need to store information unique to each thread, accessible through a common global handle. Programmers could use an associative array with the thread ID command GetCurrentThreadld, or they could use the Win32 API for organizing Thread Local Storage (TLS). The command TisAlloc calls up an integer, SLOT-ID which is the global handle for a specific TLS agreed upon by all threads, and Win32 allocates at least 64 TLS slots to each process. Unfortuneately this TLS API creates problems with code readability, because it uses SLOT-IDs rather than easily recognizable handles, and could cause memory leaks. A class called ThreadLocalStoragePtr, which addresses these issues, is presented.

Title: Architecture and Components for Data Management Security: NRL Perspective
Author(s): C.E. Landwehr and J.N. Froscher
E-mail Address: landwehr@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil
Citation: Proceedings of the 20th National Information Systems Security Conference, Oct. 1997, pp722-728
Date: Oct. 1997
Report No.: CHACS-97-052

Abstract

The DoD urgently needs system architectures that will permit the use of commercial off-the-shelf technology (COTS), including databse management systems, without making the system as a whole vulnerable to COTS shortcomings and defects. Practical architectures to meet this need will, we believe, assign security functions that require high assurance to separate, simple components, and use COTS components for the purposes for which they are developed.

The commercial sector has introduced mechanisms for access control, integrity, authentication, privacy, and non-repudiation that are designed to counter the threats to which commercial systems are subject. If the DoD can organize its systems so that there are environments where the commercial threat model holds, it may very well be appropriate to rely on the commercial mechanisms to counter those threats. However, DoD still needs to provide users with different clearances access to classified data and services at different classification levels (i.e., DoD users need multilevel secure (MLS) systems). DoD may also wish to detect and recover from the effects of subtle attacks on commercial databases, to provide cleared users with access to unclassified databases that resists traffic analysis, and to provide more secure and convenient means for maintaining user authentication to the DBMS. The balance of this position paper describes technology now being developed and/or demonstrated at NRL that provides the means to address DoD's unique security policy requirements for data management using small scale, inexpensive components in conjunction with COTS database technology.

Title: Replay and Replication Defenses Against Storage Jamming
Author(s): J.P. McDermott and J.N. Froscher
E-mail Address: mcdermott@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil
Citation: Proceedings of the 20th National Information Systems Security Conference, Oct. 1997, pp162-173
Date: Oct. 1997
Report No.: CHACS-97-053

Abstract

Storage jamming is malicious but surreptitious modification of stored data, to reduce its quality. The person initiating the storage jamming does not receive any direct benefit. Instead, the goal is more indirect, such as deteriorating the

position of a competitor. Storage jamming is an interesting problem. All the attacker has to do is occasionally write a wrong, but plausible answer. Effective attacks can occur within a single access control boundary, before encryption. Effective attacks can occur at a granularity too fine for practical audit mechanisms to detect. For this reason, these techniques alone are not generally useful in preventing storage jamming. In this paper we present examples of too important classes of storage jamming attacks: exojamming and endojamming and present too classes of defense based on detection by means other than audit.

1996 PUBLICATIONS

CHACS-96-001 Mechanical Verification of Timed Automata: A Case Study. *Myla M. Archer and Constance L. Heitmeyer*

CHACS-96-002 Implementation of IPv6 in 4.4 BSD, *Randall J. Atkinson, Daniel L. McDonald, Bao G. Phan, Craig W. Metz, and Kenneth C. Chin*

CHACS-96-003 Several Secure Store and Forward Devices, *David M. Goldschlag*

CHACS-96-004 Hiding Routing Information, *David M. Goldschlag, Michael G. Reed, and Paul F. Syverson*

CHACS-96-005 Requirements Specifications for Hybrid Systems, *Constance L. Heitmeyer*

CHACS-96-006 Automated Consistency Checking of Requirements Specifications, *Constance L. Heitmeyer, Ralph D. Jeffords, and Bruce G. Labaw*

CHACS-96-007 A Network Pump, *Myong H. Kang, Ira S. Moskowitz, and Daniel C. Lee*

CHACS-96-008 Towards a Model of Storage Jamming. *John P. McDermott and David Goldschlag*

CHACS-96-009 A Socket-based Key Management API for BSD UNIX, *Daniel L. McDonald, Bao G. Phan, and Randall J. Atkinson*

CHACS-96-010 Language Generation and Verification in the NRL Protocol Analyzer, *Catherine A. Meadows*

CHACS-96-011 Analyzing the Needham-Schroeder Public Key Protocol: A Comparison of Two Approaches, *Catherine A. Meadows*

CHACS-96-012 An Implementation of the Pump: The Event Driven Pump, *Bruce Montrose and Myong H. Kang*

CHACS-96-013 The RS-232 Character Repeater Refinement and Assurance Argument, *Andrew P. Moore and Charles N. Payne Jr.*

CHACS-96-014 Increasing Assurance with Literate Programming Techniques, *Andrew P. Moore and Charles N. Payne Jr.*

CHACS-96-015 An Analysis of the Timed Z-Channel, *Ira S. Moskowitz, Steven J., and Myong H. Kang*

CHACS-96-016 Limitations on Design Principles for Public Key Protocols, *Paul F. Syverson*

CHACS-96-017 TAME: A Specialized Specification and Verification System for Timed Automate, *Myla M. Archer and Constance L. Heitmeyer*

CHACS-96-018 Agent Safety and Security, *David M. Goldschlag, Carl E. Landwehr, and Michael G. Reed*

CHACS-96-019 A Case Study of Two NRL Pump Prototypes, *Myong H. Kang, Ira S. Moskowitz, Bruce Montrose and James Parsonese*

CHACS-96-020 A Framework for MLS Interoperability, *Myong H. Kang, Judith N. Froscher and Ira S. Moskowitz*

CHACS-96-021 Proxies for Anonymous Routing, *Michael G. Reed, Paul F. Syverson, and David M. Goldschlag*

CHACS-96-022 Legal Aspects of ICE-PICK Testing, *Bruce Gabrielson*

CHACS-96-023 Position Statement for New Paradigms for Internetwork Security Panel, *Steven Greenwald*

CHACS-96-024 Architectural Considerations for Mobile Mesh Networking, *Scott M. Corson, Joseph P. Macker, and Steven G. Batsell*

CHACS-96-025 IVOX - The Interactive VOice eXchange Application, *Brian R. Adamson and Joseph P. Macker*

CHACS-96-026 Controlled Link Sharing and Quality of Service Data Transfer for Military Internetworking, *Joseph P. Macker*

CHACS-96-027 Reliable Multicast Data Delivery for Military Networking, *Joseph P. Macker, J. Eric Klinker, and Scott M. Corson*

CHACS-96-028 Multicast Tree Construction in Directed Networks, *J. Eric Klinker*

CHACS-96-029 What is an Attack on a Cryptographic Protocol? *Paul F. Syverson*

CHACS-96-030 A New Security Policy for Distributed Resource Management and Access Control, *Steven J. Greenwald*

CHACS-96-031 Requirements and Approaches for a Computer Vulnerability *Data Archive, Bruce C. Gabrielson, Jeff D. Humphrey, and Carl E. Landwehr*

CHACS-96-032 "OR/SM" A Prototype Integrated Modeling Environment Based on Structured Modeling, *Gordon P. Wright, Radha V. Mookerjee, Radha Chandrasckharan, N. Dan Worobetz, and Myong H. Kang*

CHACS-96-033 Consistency Checking of SCR-Style Requirements Specifications, *Constance L. Heitmeyer, Bruce Labaw, and Daniel Kiskis*

CHACS-96-034 The Effects of Storage Jamming in Distributed Simulations, *John P. McDermott*

CHACS-96-035 A New Look at an Old Protocol, *Paul F. Syverson*

CHACS-96-036 A Logical Approach to Multilevel Security of Probabilistic Systems, *James W. Gray III. and Paul F. Syverson*

CHACS-96-037 A General Theory of Composition for a Class of Possibilistic' Properties, *John D. McLean*

CHACS-96-038 Formal Methods for Real Time Computing, *Constance L. Heitmeyer and Dino Mandrioli (eds)*

CHACS-96-039 Formal Methods for Real-Time Computing: A Overview, *Constance L. Heitmeyer and Dino Mandrioli*

CHACS-96-040 Formal Methods for Verifying Real-Time Systems Using Timed Automatation in Trends in Formal Methods for Real-Time Computing, *Constance L. Heitmeyer and Nancy Lynch*

1995 PUBLICATIONS

CHACS-95-001 Epistemology of Information Flow in the Multilevel Security of Probabilistic Systems, *James W. Gray, III*

CHACS-95-002 Software Requirements: A Tutorial, *Stuart R. Faulk*

CHACS-95-003 Security for the Internet Protocol, *Randall J. Atkinson*

CHACS-95-004 External COMSEC Adaptor Software Engineering Methodology, *Andrew Moore, Eather Chapman, et al.*

CHACS-95-005 A Data Pump for Communication, *Myong H. Kang and Ira S. Moskowitz*

CHACS-95-006 Improving Inter-Enclave Information Flow for a Secure Strike Planning Application, *Judith N. Froscher, et. Al.*

CHACS-95-007 SCR*: A Toolset or Specifying and Analyzing Requirements, . *Heitmeyer, A. Bull, C. Gasarch, and B. Labaw*

CHACS-95-008 A Network Pump, Myong Kang, *Ira S. Moskowitz and Daniel C. Lee*

CHACS-95-009 Storage Jamming, *John McDermott and David Goldschlag*

CHACS-95-010 One Time Passwords In Everything (OPIE): Experiences with Building and Using Strong Authentication, *Daniel L. McDonald, R. J. Atkinson, and C. Metz*

CHACS-95-011 High Assurance Computer Systems: A Research Agenda, America in the Age of Information, *John D. McLean and C.L. Heitmeyer*

CHACS-95-012 Applying the Dependability Paradigm to Computer Security, *Catherine A. Meadows*

CHACS-95-013 Using Temporal Logic to Specify and Verify Cryptographic Protocols (Progress Report), *James W. Gray, III and J.D. McLean*

CHACS-95-014 The NRL Protocol Analyzer: An Overview, *Catherine A. Meadows*

CHACS-95-015 Formal Verification of Cryptographic Protocols: A Survey, *Catherine Meadows*

CHACS-95-016 Integrity in Multilevel Secure Database Management Systems, *Catherine A. Meadows and Sushil Jajodia*

CHACS-95-017 Inference Problems in Multilevel Secure Database Management Systems, *Sushil Jajodia and Catherine Meadows*

CHACS-95-018 The Role of Trust in Information Integrity Protocols, *Gustavus Simmons and Catherine Meadows*

CHACS-95-019 The Modulated-Input Modulated-Output Model, *Ira S. Moskowitz and Myong Kang*

CHACS-95-020 Reduction of a Class of Fox-Wright Psi Functions for Certain Rational Parameters, *Allen R. Miller and Ira S. Moskowitz*

CHACS-95-021 A Network Version of the Pump, *Myong H. Kang, Ira S. Moskowitz and Daniel C. Lee*

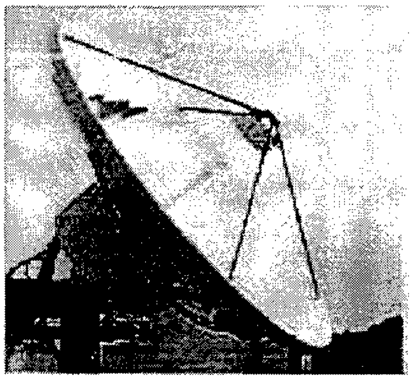
CHACS-95-022 Assurance Mappings, A Chapter of the Handbook for the Computer Security Certification of Trusted Systems, *J. McHugh, C.N. Payne, and C. Martin*

CHACS-95-023 Security Policy Model , A Chapter of the Handbook, for the Computer Security Certification of Trusted Systems, *Charles N. Payne*

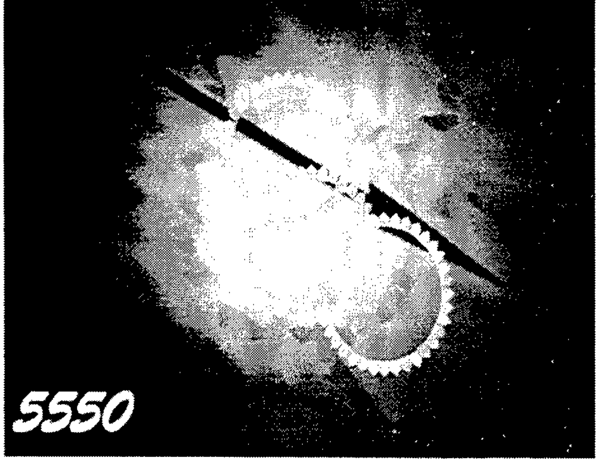
CHACS-95-024 The Epistemic Representation of Information Flow Security in Probabilistic Systems, *Paul F. Syverson and James W. Gray, III*

CHACS-95-025 Fail Stop Protocols: An Approach to Designing Secure Protocols, *Li Gong and Paul F. Syverson*

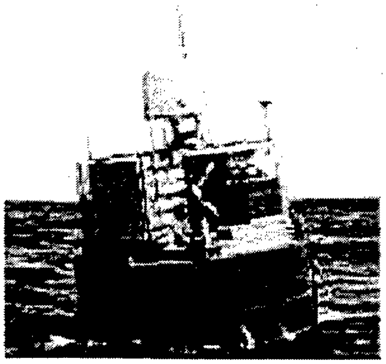
The Transmission Technology (TT) Branch conducts a research and development program directed toward the improvement of information transmission and reception between surface, air, submerged and space platforms. The Branch mission includes understanding and developing approaches to satisfy the need for affordable, efficient and robust dissemination of combat management information. In support of this goal, the Branch investigates all aspects of the process of information transfer including the development of state-of-the-art transmission equipment as well as research into antennas and channel propagation phenomena.



Transmission Technology



code 5550



Emphasis is placed on those aspects of transmission technology that permit adaptation to inhospitable natural or man-made environments. In addition, the Branch conducts research and development in support of signal intercept and related intelligence system projects. Areas of activity include: (1) wideband HF architecture and RF system engineering; (2) communication channel characterization including Arctic communication issues; (3) intercept system analysis, development, and prototype evaluation; (4) satellite and space communication technology; and (5) research into wideband and compact antenna systems.

TRANSMISSION TECHNOLOGY

CODE 5550

Title: Demonstration of High Data Rate and Medium Data Rate VSAT Communications using the Global Broadcast System (GBS) Transponder
Authors: M. Rupar, T. Krout, and A. Eley
E-mail Address: rupar@itd.nrl.navy.mil or krout@itd.nrl.navy.mil or eley@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5550--97-7921
Date: March 29, 1997
Report No.: TT-97-001

Abstract

During the months of November and December 1996, the Naval Research Laboratory (NRL) successfully demonstrated medium data rate (160 kbps) and high data rate (1.288 Mbps and higher) satellite links using transponders for the Global Broadcast System (GBS) and Joint Broadcast System (JSB). The demonstration was conducted at NRL with assistance from the Defense Information Systems Agency (DISA) and the Operational Support Office (OSO). Direct sequence spread spectrum (DSSS) links and conventional QPSK (1.544 Mbps) links were established on a satellite transponder that was simultaneously occupied with the GBS broadcast originating at the GBS earth station terminal at the Pentagon. The DSSS signal was transmitted using a very-small-aperture-terminal (VSAT) having a 24" articulated antenna, and was received by the 3.7 m earth station. The conventional QPSK signal was transmitted from the earth station was received by the VSAT. Test results showed that the satellite transponder could support the broadcast, a conventional QPSK signal and a DSSS signal simultaneously. Bit error rates in the 10-6 to 10-8 range were achievable.

Title: Theoretical and Experimental Investigation of the Impedance of a Vertical Monopole over Perfect, Imperfect, and Enhanced Ground Planes
Author(s): Michael A. Rupar
E-mail Address: rupar@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5550--97-7941
Date: April 30, 1997
Report No.: TT-97-002

Abstract

The impedance characteristics of a vertical monopole over an imperfect ground are investigated theoretically and experimentally. An expression for the change in antenna input impedance from an imperfect to a perfect ground, ΔZ, is introduced, and is used to generate results which illustrate the effects of ground constants (the earth's conductivity and relative dielectric constants) on the input impedance of a vertical monopole. Calculated results are presented correlating the change in impedance to varying ground conditions and extended to the inclusion of a radial ground screen. Theoretical analysis is compared with ground constant measurements that were conducted at three locations around the Washington, DC, area. Antenna impedance measurements were performed on monopoles of various heights at one of the surveyed locations, and at the Naval Research Laboratory's Brandywine Test Facility.

Title: Voice Processing Techniques for C4I Applications
Authors: G.S. Kang, L.J. Fransen, T.M. Moran, and D.A. Heide
E-mail Address: kang@itd.nrl.navy.mil or fransen@itd.nrl.navy.mil or moran@itd.nrl.navy.mil or heide@itd.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5550--97-9852
Date: September 9, 1997
Report No.: TT-97-003

Abstract

Speech communication is indispensable for conducting warfare. Since the Navy operates in diverse operating environments (over wide-open ocean areas, under water, in the air, over narrowband links, and over wideband channels), in various platforms (ships, submarines, aircraft, vehicles, and fixed plants), and under varied operational modes (two-way interactive, one-way noninteractive, secure, nonsecure, covert, and antijam), we need supporting speech processing technologies to communicate reliably in all of these possible circumstances. Accordingly, we generated seven different technologies for these applications.

These are the seven topics we investigated: (1) narrowband speech improvement by moving out-of-band speech components into the passband; (2) 48 kb/s speech with embedded (and operationally compatible) 32 kb/s speech; (3) a wideband/narrowband tandem interface, which does not degrade speech intelligibility; (4) narrowband multimedia terminal, which is capable of transmitting images or hand-sketches to improve the effectiveness of communication; (5) voice-mail compression operating at 1 kb/s; (6) speaker-specific digital telephone operating at 50 b/s; (7) new noise-canceling microphone, which has improved frequency response and noise rejection over currently used Navy microphones

Title: High Data Rate Very Small Aperture Terminal Networking in Support of the New Attack Submarine
Authors: LCDR Jeffrey L. Benson, Timothy L. Krout, Michael A. Rupar, and Mark H. Solsman
E-mail Address: krout@itd.nrl.navy.mil or rupar@itd.nrl.navy.mil or solsman@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5550--97-7988
Date: December 31, 1997
Report No.: TT-97-004

Abstract

During the months of August and September 1996, the Fixed Surveillance System (FSS) program office of the Intelligence, Surveillance and Reconnaissance (ISR) Directorate of the Space and Naval Warfare Systems Command (SPAWAR) with the assistance of the Naval Research Laboratory (NRL) successfully demonstrated a high data rate (1.288 Mbps and higher) satellite network link in support of the New Attack Submarine (NSSN) Open System Critical Item Test (OSCIT). The satellite network link was established between the Naval Ocean Processing Facility (NOPF) in Dam Neck, VA and the NSSN test facility in Newport, RI. A direct sequence spread spectrum (DSSS) link as well as a narrowband Quadrature Phase-Shift Keying (QPSK) link were established using a commercial satellite transponder. The DSSS signal was transmitted using a Very Small Aperture Terminal (VSAT) having a 0.6 m articulated antenna and was received by a COMSAT Radiation Systems Inc. (CRSI) Triband Transportable Satellite Earth Terminal. The narrowband signal was transmitted from the earth terminal and received by the VSAT. The two simplex links were combined at the network layer via a router and provided TCP/IP wide area network (WAN) connectivity between two local area networks (LAN) over which COTS/GOTS Joint Maritime Command Information System (JMCIS) network applications were executed. The results showed that a full duplex network link could be operated using the VSAT and commercial technology to support high rate WAN connectivity between ship(s) and shore.

Title: Satellite Networking using CDMA
Author(s): Michael A. Rupar
E-mail Address: rupar@itd.nrl.navy.mil
Citation: URSI National Radio Science Meeting, University of Colorado, Boulder, CO, Jan. 5-9, 1998
Date: 1997
Report No.: TT-97-005

Abstract

This paper discusses the technical issues involved in developing a high data rate satellite-based network able to support constant, variable and available bit-rate data. The challenge is to integrate disadvantaged users with small terminals into a high data-rate satallite network. One solution is to utilize spread spectrum signal processing, specifically code division multiple access, or CDMA, which allows multiple users to share the same signal bandwidth, encoding each signal so that it may be separated from the others during the de-spreading of the waveform.

There are advantages and disadvantages to the CDMA approach. CDMA signals are spread over a wide bandwidth, thereby having a low power spectral density. This facilitates the use of very small aparture terminals (VSATs) whose wide beamwidths would normally prohibit their operation on commercial satellites. In addition, CDMA is resistant to multipath fading, and has graceful performance degradation as the SATCOM link or network conditions deteriorate. However, any solution using CDMA for satellite networking must address it's inherent difficulties, such as maintaining power levels from a diverse user community, tradeoffs between processing "gain" and data rate, and non-linearities in the satellitetransponder.

The Naval Research Laboratory is examining the use of a CDMA satellite network for a number of users with varying requirements for data rate and different performance levels. The author discusses ongoing theoretical investigations at NRL and the University of Maryland, as well as field exercises examining CDMA performance over satellite channels. These include investigations into the use of open-loop and closed-loop tracking for transmitter power control, high order modulation and coding to increase spectral efficiency, and orderwire scenarios, both in-band and out-of-band, for dynamic access to the channel.

1996 PUBLICATIONS

TT-96-001 Data Telemetry and Acquisition System for Acoustic Signal Processing Investigations, *Michael A. Rupar, Joseph A. Goldstein and Timothy L. Krout*

TT-96-002 Performance Issues of ISDN Voice Communication Within the U.S. Navy, *David Heide and Lawrence Fransen*

TT-96-003 Narrowband Multimedia Briefing Device, *Thomas M. Moran and George S. Kang*

1995 PUBLICATIONS

TT-95-001 Delay, Doppler, and Amplitude Characteristics of HF Signals Received Over a 1300-km Transauroral Skywave Channel, *Leonard S. Wagner, Joseph A. Goldstein, Michael A. Rupar and Edward J. Kennedy*

TT-95-002 Channel Spread Parameters for the High-Latitude, Near-Vertical-Incidence-Skywave HF Channel: Correlation with Geomagnetic Activity, *Leonard S. WagneR, and Joseph A. Goldstein*

TT-95-003 2.4-kb/s Vocoder Based on Pitch-Synchronous Segmentation of Speech, *George S. Kang and Lawrence J. Fransen*

TT-95-004 Protocol Profiles for Near-Term ATM Usage, *Lynn M. Koffley and Donald G. Kallgren* code 5580

Advanced Information Technology

The Advanced Information Technology (AIT) Branch of the Information Technology Division develops and implements cutting edge hardware and software solutions to Navy problems in a number of application areas. Current research and development thrusts include:

- parallel and distributed hardware, software and display technologies;

- novel signal processing techniques directed primarily toward the exploitation of massively parallel systems;

- development of hardware-independent systems for developing and porting code for parallel processing systems;

- design and implementation of reactive and interactive control systems;

- development of technologies for decision support systems and prototyping of all varieties of decision systems including tactical decision aids and mission planning;

- exploration and demonstration of new methods for data management including data fusion, design and navigation of database systems, and correlation and tracking of current and historical information; and display technologies for visual management of all of the above applications.

The technical programs in the Branch include some basic research (6.1), a substantial exploratory development program (6.2), and a continuing effort to field technology through a succession of advanced technology demonstrations (6.3a). The Branch draws on expertise in computer science, mathematics, operations research, electrical engineering, and physics.

ADVANCED INFORMATION TECHNOLOGY

CODE 5580

Title: Virtual Environments for Shipboard Firefighting Training
Author(s): David L Tate, Linda Sibert and LCDR Tony King
E-mail Address: tate@ait.nrl.navy.mil
Citation: Conference Proceeding of the Virtual Reality Annual International Symposium
Date: March 1-5, 1997
Report No.: AIT-97-002

Abstract

A virtual environment (VE) of portions of the ex-USS Shadwell, the Navy's full-scale fire research and test ship, has been developed to study the feasibility of using immersive VE as a tool for shipboard firefighting training and mission rehearsal. The VE system uses a head-mounted display and 3D joystick to allow users to navigate through and interact with the environment. Fire and smoke effects are added to simulate actual firefighting conditions. This paper describes the feasibility tests that were performed aboard the Shadwell and presents the results of those tests.

Title: An Anti-Aliasing Technique for Splatting
Author(s): J. Edward Swan II, Klaus Mueller, Torsten Moller, Naeem Shareef, Roger Crawfis, Roni Yagel
E-mail Address: swan@ait.nrl.navy.mil
Citation: Proceedings of Visualization 97, pp197-204
Date: October 19-24, 1997
Report No.: AIT-97-004

Abstract

Splatting is a popular direct volume rendering algorithm. However, the algorithm does not correctly render cases where the volume sampling rate is higher than the image sampling rate (e.g. more than one voxel maps into a pixel). This situation arises with orthographic projections of high-resolution volumes, as well as with perspective projections of volumes of any resolution. The result is potentially severe spatial and temporal aliasing artifacts. Volume ray casting algorithms avoid these artifacts by employing reconstruction kernels which vary in width. Unlike ray casting algorithms, existing splatting algorithms to not have an equivalent mechanism for avoiding these artifacts. In this paper we propose such a mechanism, which delivers high-quality splatted images. Furthermore, our technique has the potential for a very efficient hardware implementation.

Title: A Non-divergent Estimation Algorithm in the Presence of Unknown Correlations
Author(s): Simon J. Julier, Jeffrey K. Uhlmann
E-mail Address: uhlmann@ait.nrl.navy.mill
Citation: Proceedings of the 1997 American Control Conference
Date: June 4-6, 1997
Report No.: AIT-97-005

Abstract

This paper addresses the problem of estimation when the cross-correlation in the errors between different random variables are unknown. A new data fusion algorithm, the Covariance Intersection Algorithm (GI), is presented. It is proved that this algorithm yields consistent estimates irrespective of the actual correlations. This property is illustrated in an application of decentralized estimation where it is impossible to consistently use a Kalman filter.

Title: Generalized Non-Standard Finite Differences and Applications to Shock Wave Simulation
Author(s): James B. Cole, Z. Jiang, K. Takayama
E-Mail Address: cole@ait.nrl.navy.mil
Citation: Proceedings of 21st International Symposium on Shock Waves
Date: July 20-25, 1997
Report No.: AIT-97-006

Abstract

It can be shown that exact finite difference schemes exist to solve some kinds of partial differential equations. There is no general rule for actually constructing these schemes, but they can sometimes be found by using what are called non-standard finite differences.

Using non-standard finite differences, it is sometimes possible to greatly improve the accuracy of finite difference algorithms without resorting to higher order approximations or using finer gridding. Although generalized non-standard finite difference algorithms are more complicated than standard ones, they are still much less computationally demanding than finer gridding or higher order finite differences.

In this paper we generalize the non-standard finite difference methodology in two and three dimensions. We give example algorithms and discuss current progress and applications to shock propagation.

Title: Design of a Tactical Communications Model Server for DIS-based Simulations
Author(s): Kevin L. Russo, William Smith, Henry Ng
E-mail Address: russo@ait.nrl.navy.mil
Citation: Proceedings of the SimTecT 97 (Published as an abstract only.)
Date: March 1997
Report No.: AIT-97-007

Abstract

The fidelity and realism of radio communications in Distributed Interactive Simulation (DIS) based simulations can be greatly increased by modeling the electromagnetic communications environment. While the DIS protocols support and encourage robust comms simulation few realtime simulations can devote the processing cycles to accurately model more than a simplistic electromagnetic environment.

This paper presents the design and implementation of a Tactical Communications Model Server (TCMS) which allows a distributed simulation application to fetch signal reception parameters for a transmission, given the transmitter/receiver's location, operating characteristics, link bandwidth allocation, and message attributes. Since the TCMS runs as a separate process from the simulation and monitors DIS network traffic, maintaining a cache of Tx/Rx results, latencies to receiver queries are minimized. The design also allows for the effects of weather and terrain to be included in connectivity calculations.

Title: Tips and Techniques for Conducting Site-distributed DIS Exercises
Author(s): Kevin L. Russo
E-mail Address: russo@ait.nrl.navy.mil
Citation: Proceedings of the SimTecT 97 (Published as an abstract only.)
Date: March 1997
Report No.: AIT-97-008

Abstract

As Distributed Interactive Simulation (DIS) exercises grow to exceed a local site's LAN processor and network capacity, simulation specialists need a quick, reconfigurable, low cost alternative to installing dedicated simulation networks to participating sites. Even when high entity counts are not the goal, linking geographically separated sites is desirable because of fixed assets like manned flight simulators which are not easily transported. In the US, large site-distributed DIS exercises have usually been run over the DoD's DSI net, and elsewhere in the world, over ISDN lines. At the heart of this approach are IP multicast and the Internet Multicast Backbone.

This paper will present a practical guide for the simulation specialist to quickly configure multiple sites into a large virtual simulation network. Specific tips, techniques and experimental data related to exercise setup, management, real-time monitoring, and post-exercise processing will be presented culled from NRL's experiences in the ARPA STOW RITN program and TTCP experiments conducted between the NRL and defense groups in Australia, Canada, and the UK.

Title: Parallelization of the Synthetic Scene Generation Model
Author(s): Becky Popp, D.A. Newman
E-mail Address: popp@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--97-9850
Date: June 1997
Report No.: AIT-97-010

Distribution of abstract and report authorized to U.S. Government agencies and their contractors.

Title: Matching Sets of 3-D Line Segments With Application to Polygonal Arc
Author(s): Behzad Kamgar-Parsi and Behrooz Kamgar-Parsi
E-mail Address: behzad@ait.nrl.navy.mil
Citation: IEEE Transaction Pattern Analysis and Machine Intelligence, v19, n10, pp1090-1099
Date: October 1997
Report No.: AIT-97-011

Abstract

In this paper we consider two sets of corresponding 3-D line segments of equal length. We derive a closed-form solution for the coordinate transform (rotation and translation) that gives the best match between the two sets; best in the sense of a least-squares distance measure between the sets. We use these results as the basis to construct efficient algorithms for solving two fundamental problems in computer vision. One is the problem of matching polygonal arcs, particularly, the problem of finding a match between a short arc and a piece of a long arc. The second problem is finding the best match between a set of edge fragments (extracted from sensor data) and the corresponding edges of a prestored model.

Title: An Introduction to the Processing Graph Method
Author(s): David J. Kaplan
E-mail Address: kaplan@ait.nrl.navy.mil
Citation: Proceedings of IEEE International Conference Workshop on Engineering of Computer Based Systems
Date: March 24-28, 1997
Report No.: AIT-97-013

Abstract

The Processing Graph Method (PGM) technology is a paradigm that provides the engineer/system designer with an environment to specify and maintain applications in a form which is invariant over a wide range of MIMD message passing parallel architectures.

We will give the reader the flavor of this approach by providing a description of an application; illustrating how that application is represented; showing typical results obtained by running the application; providing a short description of the atoms that are used to build the application; and providing a short discussion of the technical issues to which PGM must respond.

Title: High Accuracy Solution on Maxwell's Equations Using Non-Standard Finite Differences
Author(s): James Cole
E-mail Address: cole@ait.nrl.navy.mil
Citation: Computer in Physics, v11, n3, May/June 1997, pp287-292
Date: May/June 1997
Report No.: AIT-97-014

Abstract

We introduce a new finite-difference time-domain algorithm to directly solve Maxwell's equations based on non-standard finite differences. This algorithm is some 10,000 times more accurate than the standard one on a coarse grid. Although computational load per grid point is greater, it is more than offset by a large reduction in the total number of grid points needed to solve a given problem. In addition, algorithm stability is greater so that the number of iterations needed is also reduced. While optimum performance is achieved at a fixed frequency, the accuracy is still higher than that of the standard algorithm over "moderate" bandwidths.

We have implemented the algorithm in FORTRAN 90 and can easily model spatially variant media and irregular boundaries. By displaying one or more fields per waveperiod we obtain on-line movie-like visualizations of the electromagnetic fields while the computation is running.

Title: Simulation of Organizational Workflows for the Quantitative Evaluation of Business Processes
Author(s): Raymond L. Woodward, William R. Smith, Susan K. Numrich, and Douglas A. Comery
E-mail Address: smith@ait.nrl.navy.mil
Citation: Proceedings of 1997 Simulation Multiconference
Date: April 6-10, 1997
Report No.: AIT-97-015

Abstract

Business outcomes ultimately relate to human performance, organizational relationships and inputs. In this work the example is used of an international collaborative scientific program to demonstrate the ability to realistically model organizational behavior and to estimate the effect of business processes on outputs and effectiveness. Organizational linkages were mapped, flow charts developed to describe operational activities, and outputs were quantified. The organization was populated and equations written based on both experience and polling, to relate activity to outputs. In a spreadsheet format the equations were integrated in a simulation of the annual cycle of operations. Sensitivity was assessed by the comparison of outputs using "optimistic" and "typical"

parameters to characterize work patterns and human response, and ground truth was provided by a comparison against current measured performance. The method was then used to examine alternative structures and ways of doing business. The advantages of modeling were in the discipline it provides and the structured approach to thinking through business processes. The quantitative outputs provide a clear basis for decision making. The work describes the approach to establishing the model and solution method, the visualization and mathematical description of human activity, and the problems of output measurement. An organizational model is of no value if it does not have the power to influence organizational decisions, and the politics of achieving acceptance can over-ride the effort in developing and using the tools themselves. Selling the process is part of selling the results.

Title: Challenges In Virtual Reality
Author(s): Lawrence J. Rosenblum and Robert A. Cross
E-mail Address: rosenblum@ait.nrl.navy.mil
Citation: Book, Chapter 18, Academic Press, pp325-339
Date: 1997
Report No.: AIT-97-018

Abstract

Virtual reality (VR) is a demanding computer science research field. This paper discusses important problems faced in current virtual reality research in its attempt to provide 3D interaction, visual realism, physical realism, and multisensory immersion. We also examine selected applications to provide a sense of what is achievable today in VR and the directions in which the field is heading.

Title: VR Systems: Out from the Laboratory
Author(s): Lawrence J. Rosenblum
E-mail Address: rosenblum@ait.nrl.navy.mil
Citation: Proceedings of the Virtual Reality and Multimedia 97 Conference
Date: September 10-12, 1997
Report No.: AIT-97-020

Abstract

In spite of the large amount of "hype" that accompanied virtual reality (VR) earlier this decade, the field has produced only a few examples of demonstrably useful systems. Systems must be fielded and validated to show that VR is useful for purposes other than academic research. This paper discusses two VR systems developed at the Naval Research Laboratory that have received validation by statistical analysis or by user acceptance. One system focuses on experiments in shipboard firefighting to verify the effectiveness of VR as a mission planning tool. Using trained U.S. Navy firefighters, we conducted a shipboard experiment. The VR-trained firefighters performed significantly better on both navigation and firefighting tasks. The second system involved developing and application using NRL's VR Responsiveness Workbench to provide situational awareness inside a U.S. Marine Corps combat operation center (COC). This system has been called a major advance that is likely to eliminate paper maps in the COC.

Title: The Processing Graph Method Tool (PGMT)
Author(s): Richard S. Stevens
E-mail Address: stevens@ait.nrl.navy.mil
Citation: Proceedings of The ASAP 97 Conference
Date: July 14-16, 1997
Report No.: AIT-97-021

Abstract

To acquire state-of-the-art hardware at reduced cost, the US Navy is committed to buying Commercial Off The Shelf (COTS) computer hardware. In this rapidly changing technological world, today's hardware will be obsolete tomorrow. The Navy's complex problems often require more computational power than can be delivered by a single serial processor. The solution lies in distributed processing. However, distributed processors tend to have architecture specific languages, requiring an expensive and time-consuming manual rewrite of application software as new technology and new machines become available.

The Processing Graph Method[3] (PGM) developed at the Naval Research Laboratory (NRL) in Washington, DC, is an architecture independent method for specifying application software for distributed architectures. Its model of computation is reconfigurable dynamic data flow: dynamic, because the amount of data consumed and produced by an actor may vary from one firing to another, and reconfigurable, because a graph may be disassembled and reassembled. PGM was implemented on the Navy Standard Signal Processor (AN/UYS-2), and on VAX and Sun workstations. The PGMT project at NRL is developing a tool set that will facilitate the implementation of PGM on a given distributed architecture at relatively low cost. We describe the major features PGM and discuss the PGMT project.

Title: Applying Simulation Based Virtual Reality for Surface Combatant Training
Author(s): Henry Ng, Ali Farsaie, Les Elkins
E-mail Address: ng@ait.nrl.navy.mil
Citation: Proceedings of the 19th Interservice/Industry Training Systems and Education Conference (I/ITSEC)
Date: December 2-4, 1997
Report No.: AIT-97-023

[3] See the PGMT home page at http://www.ait.nrl.navy.mil/pgmt/pgm2.html for further information.

Abstract

In current shore-based surface combatant training, new crews are trained using real combat consoles in a classroom environment. This approach has disadvantages that include the considerable expense of supporting, maintaining, and reconfiguring the real consoles used in theses facilities. As visual simulation and virtual reality have increased in capability and decreased in cost, these technologies can provide cost-effective solutions for training. The Naval Research Laboratory is currently using virtual reality, simulation, and multimedia tools to develop a Distributed Synthetic Combat Information Center (CIC) for the surface ship training. The goal of the project is to create a distributed, immersive virtual reality system to complement current training capability. It will allow surface ship CIC crew members at different geographical locations to perform team training in a virtual ship environment. The virtual environment offers a true interactive 3D view of the interior of the CIC. This system will provide the feeling of real presence for surface ship combatant crews in a realistic combat engagement atmosphere instead of a classroom-like environment. It also simulates the equipment that the crew can interact with to perform detection, classification and target engagement activities. Information visualization will aid students in learning different tactical deployment of the combat systems. Intelligent agents will be used to compensate for different educational levels of recruits and to reduce the number of instructors. The system will accommodate geographically distributed sites and provide high system availability. The virtual CIC's network capability will be implemented through a High Level Architecture (HLA) federate: crew members within the Federation Object Model (FOM) will communicate with each other, and a FOM representing the entire ship's CIC can participate in HLA exercises. This paper will describe the project requirements, technical approach, system tradeoffs, current accomplishments and future direction.

Title: The Virtual Reality Responsive Workbench: Applications and Experiences
Author(s): Lawrence Rosenblum, Robert Doyle, and James Durbin
E-mail Address: rosenblum@ait.nrl.navy.mil
Citation: Proceedings of the British Computer Society Conference on Virtual Reality, Networking, and the WWW
Date: April 15-17, 1997
Report No.: AIT-97-024

Abstract

Virtual reality (VR) is a complex and challenging field [Earnshaw and Rosenblum, 1995; Rosenblum and Cross, 1997] and several distinct types of systems have been developed for displaying and interacting with virtual environments. One of the newest is the Virtual Reality Responsive Workbench [Kreuger and Froehlich, 1994; Kreuger et al., 1995; Rosenblum, Bryson, and Feiner, 1995]. The Workbench is an interactive VR environment designed to support a team of end users such as military/civilian command and control

specialists, designers, engineers, and doctors. The Virtual Workbench creates a match for the "real" work environment of persons who would typically stand over a table or a workbench as part of their professional routine. For example, the Workbench could be used to represent fluid flow over ship's hull while supporting a design team in interactive visualization. Perhaps the greatest strength of the VR Responsive Workbench is the ease of natural interaction with virtual objects. Current interactive methods emphasize gesture recognition, speech recognition, and a simulated "laser" pointer to identify and manipulate objects.

This paper classifies VR systems into three categories: immersive head-mounted displays (HMD's), immersive non-HMD systems; and non-immersive table top systems. We discuss the utility of each classification. Several applications that we developed in the Virtual Reality Laboratory of the Information Technology Division (ITD), Naval Research Laboratory (NRL) are examined and we discuss our experiences with VR Responsive Workbench interfaces and software architecture.

Title: A Communication Modeling Approach For Advanced Distributed Simulation
Author(s): William Smith, Henry Ng, and Karl Washburn
E-mail Address: smith@ait.nrl.navy.mil
Citation: Proceedings of the SPIE 11th Aerosense Symposium
Date: April 20-25, 1997
Report No.: AIT-97-025

Abstract

NRL is developing an end-to-end distributed simulation environment in support of several Navy technology development programs. One of the critical needs in this distributed simulation environment is a tactical communications emulator. Current distributed simulation exercises seldom provide a flexible communications system model with realistic fidelity. As a result, we are creating a Tactical Communications Model Server architecture which operates in Advanced Distributed Simulations (ADS). We are taking an evolutionary approach that will allow integration of specialized or general Commercial Off-the-Shelf (COTS) communication connectivity models. This paper describes our objectives, the system architecture and design trade-off considerations.

Title: Matching 3-D Arcs
Author(s): Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi
E-mail Address: behzad@ait.nrl.navy.mil
Citation: Proceedings of the IEEE Conference on Computer Vision Pattern Recognition (CVPR-97), pp28-33
Date: June 17-19, 1997
Report No.: AIT-97-026

Abstract

We present a new algorithm for efficient matching of 3-D polygonal arcs. The algorithm is based on the decomposition of the arcs into sets of corresponding line segments with equal lengths. We derive a closed-form solution for the transformation that gives the best match between two sets of corresponding line segments (best in the sense of an L_2 norm distance measure), which enables the development of an efficient arc matching algorithm. We apply this algorithm to the problem of finding a match between a short arc and a piece of a long arc in real and synthetic images, and compare the results with alternative techniques in the literature.

Title: A Sub Optimal Algorithm For Automatic Map Building
Author(s): Michael Csorba, Jeffrey Uhlmann, Hugh F. Durrant-Whyte
E-mail Address: uhlmann@ait.nrl.navy.mil
Citation: Proceedings of the 1997 American Control Conference (ACC)
Date: June 4-6 , 1997
Report No.: AIT-97-027

Abstract

This paper examines the problem of automatically constructing a map of an unknown environment from a vehicle whose location is also unknown. The application of the Kalman filter to this problem is briefly described and the practical limitation of the filter in this context is discussed. A suboptimal algorithm, the Relative filter, is introduced that avoids many of the computational and practical problems of the direct Kalman filter approach to this problem. The performance of the full Kalman filter and the Relative filter is compared in a real map building scenario.

Title: Situational Awareness Using the VR Responsive Workbench
Author(s): Larry Rosenblum, Jim Durbin, Robert Doyle, Rob King, David Tate
E-mail Address: rosenlbum@ait.nrl.navy.mil, durbin@ait.nrl.navy.mil, tate@ait.nrl.navy.mil
Citation: IEEE Computer Graphics Society, v16, n4, pp12-13
Date: July 1997
Report No.: AIT-97-028

This published article has no abstract.

Title: Applying Morphological Filters to Acoustic Broadband Correlogram
Author(s): Haw-Jye Shyu
E-mail Address: shyu@ait.nrl.navy.mil
Citation: Proceedings of IEEE International Conference on Systems, Man and Cybernetics
Date: October 12, 1997
Report No.: AIT-97-029

Abstract

An Acoustic broadband correlogram, a two dimensional display over time of the cross-correlation of signals received by a two-sensor system, is often used to detect targets close to the sensor system. Often, the correlogram is cluttered by the strong interface generated by distant and yet strong sources. These strong interferers appear in the form of dark vertical and nearly-vertical lines in the broadband correlogram and hinder the detection of nearby targets. This paper presents an automatic target detection system for broadband acoustic correlograms designed to take into account the interference from strong sources. The system consists of three parts: (1) a pre-processing stage, (2) a Delay Curve Hough Transform (DCHT) and (3) an onion peeling process. The pre-processing stage consists of a morphological filter (the rolling arc) and a linear histogram stretching process to improve the contrast of the morphologically filtered correlogram. The modified Hough Transform, based on the assumption that the target moves with constant velocity, is designed to detect *delay curves* in the broadband correlograms. Finally, the onion peeling process is an iterative process that sequentially removes the strongest detected *delay curve* from the correlogram and feeds the modified correlogram back to the Hough Transform to detect the next strongest *delay curve*.

Title: Optimum Laplacian for Digital Image Processing
Author(s): Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Azriel Rosenfeld
E-mail Address: behzad@ait.nrl.navy.mil
Citation: Proceedings of the International Conference on Image Processing (ICIP'97), v2, pp728-731
Date: October 26-29, 1997
Report No.: AIT-97-031

Abstract

Spatially quantized approximations of the Laplacian used in digital image processing are not rotationally invariant. We examine the anisotrophy of 3x3 Laplacian operators for images quantized in square pixels, and derive, from optimizing criteria, the operator which has the minimum overall anisotropy.

Title: Registration Algorithms for Geophysical Maps
Author(s): Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi
E-mail Address: behzad@ait.nrl.navy.mil
Citation: Proceedings of IEEE Oceans' 97 Conference, pp. 974-980
Date: October 6-9, 1997
Report No.: AIT-97-032

Abstract

Map making surveys conducted underwater, where access to GPS is not available, can incur significant positional inaccuracies. To obtain accurate geophysical maps (e.g. seafloor elevation map, gravity map) for use in high precision navigation positional inaccuracies need to be corrected by registering overlapping surveys. In this paper, we present an algorithm for automatic registration of overlapping data patches. The matching primitives we use in the registration algorithm are contours of constant field value. This makes it possible to apply the algorithm to regions where map features (peaks, ridges, etc.) are scarce. The basic structure of the algorithm is similar to that developed previously in [7]. The new algorithm, however, improves upon the previous technique in several ways, including a new technique for efficient contour matching and a closed-form solution for the optimum transformation. These improvements make the registration more accurate and computationally less intensive. We demonstrate the efficacy of the algorithm on synthetic gravity data.

Title: Collaborative Decision Making Between The Federal Aviation Administration and The Air Transport Industry
Author(s): Patrick Gorman, James B. Hofmann
E-mail Address: hofmann@ait.nrl.navy.mil, gorman@ait.nrl.navy.mil
Citation: 16th DASC Proceedings
Date: October 26, 1997
Report No.: AIT-97-033

Abstract

The RTCA Task Force on Free Flight Implementation recommended 35 near term improvements to the current National Airspace system, suggesting the highest return, lowest cost items be addresses first. The rate of return on Collaborative Decision Making (CDM) has been conservatively estimated at 500:1.

A software product called Flight Schedule Monitor (FSM), was built to display real-time airport loading using ATMS (Air Traffic Management System) input, generate and model outcomes of possible solutions to overloading, and encourage improved communications. Communications between the FAA and the Airline Operations Centers (AOCs) are passed via the “AOCnet”-- a high speed digital network.

Several other recommendations of the RTCA committee will be addressed using the same network to transmit traffic density, Special Use Airspace Status, unusual weather conditions and airline information affecting NAS operations, among other information.

The value of CDM probably lies as much in process and potential as what has already been accomplished.

Title: The Real-Time Retargeting Distributed Simulation TestBed
Author(s): Karl Washburn, Henry Ng
E-mail Address: washburn@ait.nrl.navy.mil, ng@ait.nrl.navy.mil
Citation: Proceedings of the 2nd ASNE Modeling, Simulation and Virtual Prototyping Conference
Date: November 24-25, 1997
Report No.: AIT-97-034

Abstract

NRL is developing and applying Modeling and Simulation (M&S) technologies in support of the Real-Time Retargeting Accelerated Capabilities Initiative (RTR/ACI) for the Office of Naval Research (ONR). Real-Time Retargeting is a concept in which Naval tactical air strike assets are wholly or partially reassigned, while in flight, to strike newly emergent or time-critical targets. The RTR/ACI is developing new technologies to support such operations. Within the ACI program, a modeling and simulation component has been established to integrate and assess the performance of those technologies in a realistic environment and to explore various RTR concepts of operation with both hardware and humans in the loop.

This paper describes our research objectives in developing the RTR Distributed Simulation Testbed. We discuss the RTR concept, the ACI and our simulation approach within it. We describe the system architecture, and the major components are introduced and their integration discussed.

Title: A Tactical Communications Modeling Approach For Advanced Distributed Simulation
Author(s): Karl B. Washburn, Henry C. Ng, Carol Pawlowski
E-mail Address: washburn@ait.nrl.navy.mil, ng@ait.nrl.navy.mil
Citation: Proceedings of the 2nd ASNE Modeling, Simulation and Virtual Prototyping Conference
Date: November 24-25, 1997
Report No.: AIT-97-035

Abstract

NRL is developing an end-to-end distributed simulation environment in support of Navy technology development programs. One of the critical needs in this environment is tactical communications emulation. Current distributed simulation exercises seldom provide a flexible communications system model with realistic fidelity. As a result, we are creating a Tactical Communications Model Server which operates in Advanced Distributed Simulations (ADS). We are taking an evolutionary approach which allows integration of standalone communications modeling toolkits into distributed exercises. Concurrently, we are developing a Message Handler to act as an interface between specific simulation network protocols and communications-capable entity simulations. This paper describes our objectives in creating these distributed simulation components, their design considerations, and their architectures.

Title: Incorporating Realistic Environmental Effects Into Distributed Interactive Simulation
Author(s): Jerry Gorline
E-mail Address: gorline@ait.nrl.navy.mil
Citation: Proceedings of the 2nd ASNE Conference
Date: November 1997
Report No.: AIT-97-037

Abstract

The Naval Research Laboratory's (NRL) Advanced Information Technology (AIT) Branch is conducting research to advance the state-of-the-art technology for distributed simulation. One of the activities is to incorporate realistic environmental effects in distributed simulation exercises. The weather can play a major role in the outcome of real battles. The inclusion of interactive environmental effects is necessary to achieve a realistic battle simulation. Recognizing this, AIT is incorporating environmental effects into the Advanced Multi-Warfare Assessment and Research System (Advanced MARS), a distributed Naval engagement simulation system.

Most distributed simulation exercises conducted either assume perfect environmental conditions or do not take into account environmental effects on the system performance. The Modeling and Simulation (M&S) community is currently developing methods to incorporate realistic environmental effects into existing and emerging distributed simulation systems.

In the Advanced MARS model, a weather manager will intercept data periodically from the Total Atmosphere Ocean Server (TAOS) when an update is needed. Data gathered from the Master Environmental Library (MEL) will be distributed to the model by TAOS. The weather data will be distributed to various weather objects in the Area of Interest (AOI). These weather objects will be capable of dynamically interacting with other simulation entities. Examples include a wind field object altering the course of an airborne entity, a haze object degrading the performance of an electro-optic or infrared (EO/IR) sensor, a rain object slowing down the movement of ground forces and a high sea-state hindering an amphibious assault.

Title: Using Virtual Environments To Train Firefighters
Author(s): David L. Tate, Linda E. Sibert, LCDR Tony King
E-mail Address: tate@ait.nrl.navy.mil
Citation: IEEE Computer Graphics and Applications, v17, n6, pp23-29
Date: November 1997
Report No.: AIT-97-039

Abstract

Virtual reality (VR) is an emerging technology that currently gets the most visibility when used for entertainment purposes, but there is also much research under way to try to harness this new technology for more productive means. The U.S. Navy is interested in determining how VR can be used to teach its sailors and officers how to perform their jobs better. This paper describes a project at the Naval Research Laboratory to investigate the feasibility of using immersive virtual environments as a tool for shipboard firefighting training and mission rehearsal. Feasibility tests were performed aboard the ex-USS Shadwell, the Navy's full-scale fire research and test ship, and the results presented here show promise for the benefits of VR training over conventional training methods.

Title: High-resolution Underwater Acoustic Imaging with Lens-based Systems
Author(s): Behzad Kamgar-Parsi, Bruce Johnson, Don Folds, Ed Belcher
E-mail Address:behzad@ait.nrl.navy.mil
Citation: International Journal of Imaging Systems and Technology (Special Issue), v8, pp377-385
Date: 1997
Report No.: AIT-97-040
Abstract

In recent years, several sonars designed for high-resolution, short range underwater imaging have been developed. These imaging systems use an acoustic lens to focus the incoming waves on an array of transducers. In this paper we describe three prototype systems that use a line-focus or a point-focus lens, and operate at a frequency of 300 kHz or 3 Mhz. The line-focus lens produces 2D intensity images, while the point-focus lens produces 3D intensity images. We present sample images taken from moving and stationary platforms, and discuss the techniques used for processing the acoustic backscatter data to reconstruct and visualize the scene. The images, particularly those taken with a point-focus lens, show a remarkable degree of detail.

Title: Virtual Environment Firefighting/Ship Familiarization Feasibility Tests
Author(s): Frederick W. Williams, Patricia A. Tatem, and CDR John P. Farley, USN; David L. Tate and Linda Sibert; LCDR Tony King,USN; Donald H. Hewitt; Charles W. Siegmann III and Jennifer T. Wong; LT Terrance A. Toomey, USN
E-mail Address: tate@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/6180--97-9861
Date: 1997
Report No.: AIT-97-042

Abstract

Virtual Environments Firefighting/Ship Familiarization Feasibility Tests were conducted on the ex-USS Shadwell. The results of these tests indicate that there are measurable gains using virtual environment (VR) training with respect to water usage and time to achieve compete extinguishment. The data also indicates gains for the time to travel from Repair 2 to the fire compartment and begin the initial attack. The time to transit from the 01 level to the fire area under reduced visibility was reduced by one-half for subject trained with VR.

Title: Nonlinear Transformation for Spatial Matched Filtering
Author(s): Yung P. Lee and Haw-Jye Shyu
E-mail Address: shyu@ait.nrl.navy.mil
Citation: The Journal of the Acoustical Society of America, v97, n5, pt. 2 (Abstract only)
Date: 1997
Report No.: AIT-97-043

Abstract

A detect-on-track algorithm based on the Hough transform has been applied to acoustic broadband correlograms for passive detection and localization. The Hough transform integrates (sums) the amplitudes along a set of delay curves of interest. The delay curves are calculated over a range of closest point of approach (CPA), speed, and heading of the targets. When normalized by the number of points, the Hough transform computes the arithmetic-mean along the track. This process is referred to as an arithmetic-sum (AS) transform. This AS transform optimally reduces the variance of the noise, but can also generate significant ambiguous side-lobes. To reduce the sidelobe, two nonlinear transforms are proposed: The logarithmic-sum (LS) transform and the harmonic-sum (HS) transform. The LS-transform sums dB's while the HS-transform sums the reciprocal of the amplitudes along the track. When normalized by the number of points, the LS transform computes the geometric-mean and the HS transform computes the harmonic-mean along the track. Simulations show that the nonlinear transforms perform the same as the AS transform in noise-limited environments but outperform the AS transform in sidelobe-limited environments.

1996 PUBLICATIONS

AIT-96-002 Beasties and Other Bots, *James B. Hofmann*

AIT-96-003 Synthetic Database Methods, *Karen A. Erner*

AIT-96-004 The Challenge of Virtual Reality, *Lawrence J. Rosenblum and Robert A. Cross*

AIT-96-005 VHDL-Based Performance Modeling for the Processing Graph Method Tool (PGMT) Environment, *Roger Hillson, David J. Kaplan. Robert Klenke, and James Aylor*

AIT-96-006 Fuzzy-Algebra Uncertainty Assessment, *J. Arlin Cooper and Douglas K. Cooper*

AIT-96-009 Estimating the Effective Depth of Laser Imaging Systems in Various Ocean Environments, *Jerry L. Gorline*

AIT-96-010 Dynamic Route Optimization with Time-Expanded Graphs, *Miguel Zuniga*

AIT-96-011 General Data Fusion for Estimates with Unknown Cross Covariances, *Jeffrey K. Uhlmann*

AIT-96-012 A Minimization Theorems for Verification Conditions, *Ward Douglas Maurer*

AIT-96-013 A Scaleable Multicast Routing Algorithm For IP-ATM-IP Networks, *Mohammed Arozullah and Stephen G. Batsell*

AIT-96-014 Underwater Imaging with Acoustic Lens: Image Processing and Visualization, *Behzad Kamgar-Parsi*

AIT-96-016 Relative Precision in the Inductive Assertion Method, *Ward Douglas.Maurer*

AIT-96-017 The Use of Partial Functions In Proving That a Program Does Not Crash, *Ward Douglas Maurer*

AIT-96-019 Localization in a Shallow Water Environment Using Inter-Array BroadBand Correlation, *Wendell L. Anderson, Haw-Jye Shyu and William R. Smith*

AIT-96-020 Acoustic Scintillations in the Straits of Florida, *F. D. Tappert, X. Tang, and Dennis B. Creamer*

AIT-96-021 Performance of Detect-on-Track in a High-Shipping Environment, *Yung P. Lee and Haw-Jye Shyu*

AIT-96-022 High-resolution Underwater Acoustic Imaging with Lens-based Systems, *Behzad Kamgar-Parsi, Bruce Johnson, Don Folds, and Ed Belcher*

AIT-96-023 FinCEN MPP, *Joseph B. Collins*

AIT-96-024 Advanced Processor Technology, *Wendell Anderson, Becky Popp, Haw-Jye Shyu, and William R. Smith*

AIT-96-025 Finite-difference Tim-Domain Simulations and Visualizations of Optical, Electromagnetic, and Acoustic Wave Propagation and Scattering in Complicated Environments, *James B. Cole, and Neelam Gupta*

AIT-96-026 Advanced Distributed Simulation, *Lawrence C. Schuette, Jeffrey M. Opper, William P. Niedringhaus, and Brian R. Winner*

AIT-96-027 ALMDS Air Task, *Jerry L. Gorline*

AIT-96-028 VR goes Legit!, *Lawrence J. Rosenblum*

AIT-96-029 Development of a Tactical Decision Aid for Shipboard Damage Control, *David L. Tate*

AIT-96-030 Strike Visualization in Stereo on the Virtual Workbench, *Ranjeev Mittu, and Jeffrey K. Uhlmann*

AIT-96-031 Shipboard VR: From Damage Control Design, *Jim Durbin, Dan Fasulo, Upul Obeysekare, Lawrence J. Rosenblum, and David L. Tate*

1995 PUBLICATIONS

AIT-95-001 Reconstruction and Visualization of Underwater Objects from High-Resolution Acoustic Lens Data, *Behzad Kamgar-Parsi and Bruce J ohnson*

AIT-95-002 Finite-Difference Time-Domain Simulations of Wave Propagation and Scattering as a Research and Educational Tool, *J. B. Cole, R. A. Krutar, S. K. Numrich, and D. B. Creamer*

AIT-95-003 Technical Documentation of Nodestar, *Lawrence D. Stone, Thomas L. Corwin, and James B. Hofmann*

AIT-95-004 Distribution and Moments of The Weighted Sum of Uniform Random Variables, With Applications In Reducing Monte Carlo Simulations, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh*

AIT-95-005 Autonomous Battle Damage Assessment Study, *Tamara Luzgin*

AIT-95-006 A High Accuracy FDTD Algorithm to Solve Microwave Propagation and Scattering Problems on a Coarse Grid, *James B. Cole*

AIT-95-007 Tactical BDA for Space and Electronic Warfare (abstract only), *Tamara Luzgin*

AIT-95-008 Threat Site Overflight Modeling for Strike Route Optimization, *Miguel R. Zuniga and Patrick Gorman*

AIT-95-009 Hyperbolic Pattern Detection Using the Hough and Fourier Transform, *Becky Popp*

AIT-95-010 Persistence in Computational Geometry, *Ali R. Boroujerdi*

AIT-95-012 Virtual Reality, Visualization and Their Application, *Rae E. Earnshaw and Lawrence J. Rosenblum*

AIT-95-013 Interactive Realism for Visualization Using Ray Tracing, *Robert A. Cross*

AIT-95-014 Infrastructure for Rapid Execution of Strike-Planning Systems, *James B. Hofmann, John Cleary, Darrin West, Larry Mellon, and Jim Ramsey*

AIT-95-015 Effectiveness of Various New Bandwidth Reduction Techniques in ModSAF, *Kevin L. Russo, Lawrence C. Schuette, Ph.D., Joshua E. Smith, and Matthew McGuire*

AIT-95-016 Network Routing Models Applied to Aircraft Routing Problems, *Zhiqiang Chen, Andrew T. Holle, Bernard M.E. Moret, Jared Saia, and Ali Boroujerdi*

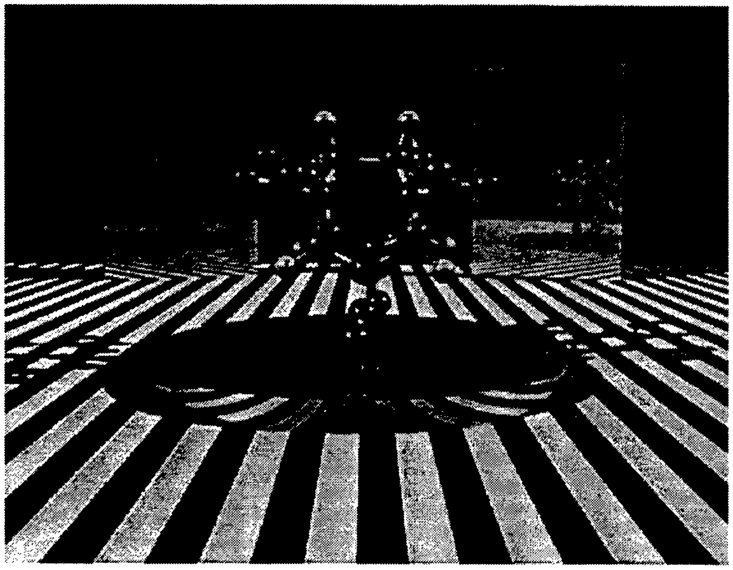
AIT-95-017 High Accuracy Solution of Maxwell's Equations Using Non-Standard Finite Differences, *James B. Cole*

AIT-95-018 Coding and Compression with Flexible Transform, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Lawrence C. Schuette*

AIT-95-019 Virtual Reality: Research Issues and Applications, *Robert A. Cross and Lawrence J. Rosenblum*

AIT-95-020 Persistent Linked Structures at Constant Worst-Case Cast, *Ali R. Boroujerdi and Bernard M.E. Moret*

AIT-95-021 Estimating the Effective Depth of Laser Imaging Systems in Various Ocean Environments, *Jerry L. Gorline*



Center For Computational Science

code 5590

The Center for Computational Science (CCS), Code 5590, conducts research and development to further the advancement of computing and communications systems to solve Navy problems. The Branch accomplishes this mission through a balanced focus on service, research, and development. The Center is committed to investigating and developing leading edge technologies to establish an advanced computational environment that will benefit all research areas. The Branch studies new technologies to evaluate their potential. Promising technologies are further developed, enhanced, and transitioned to production systems. The Branch's operational efforts provide for a computing environment that emphasizes reliability, high performance, and user productivity. In the area of research and development the Branch develops and implements new technologies, both hardware and software, to solve Navy problems in diverse application areas. Current thrusts include: parallel and distributed hardware, software and display technologies; signal processing techniques directed toward exploitation of massively parallel systems; development of hardware architecture independent systems for developing and porting code for parallel processing; and development of high-speed networks.

In the area of operational support, the Center provides shared high performance computing and networking resources and related services, including user support and training, for NRL, Navy, and DoD interdisciplinary research efforts. The Branch manages and operates NRL's shared massively parallel supercomputer, vector mini-supercomputer, central file server/archiver, and scientific visualization systems. The Branch has responsibility for the laboratory's local area network and external connections to network and computer systems world-wide. The Branch also provides laboratory ADP logistic support by identifying ADP requirements and securing and administering contractual support for lab-wide or multiple buys of ADP systems, software and services.

Title: Modes in Amorphous Silicon
Author(s): Brian Davidson, J. L. Feldman, G. E. Engel, S. R. Bickham
E-mail Address: davidson@volt
Citation: Naval Research Laboratory Report, OP/5590--97-0001, and International Workshop on Disordered Systems, Andalo, Italy
Date: March 3-6, 1997,
Report No: CCS-97-001

Abstract

We discuss how the vibrational modes in an amorphous material can be characterized by various correlation functions. The spectrum of modes can be expected to contain both extended and localized ones separated by mobility edges. The inverse participation ratio can be used as a rough measure of the degree of localization. To examine the vibrational modes in more detail, we propose to study moduli of Fourier-transforms of powers of eigenvector components. We have applied the analysis to vibrational modes of amorphous silicon. The structural and potential models we use are based on the Wooten-Winer-Weairc bond-switching algorithm and Stillinger-Weber classical potential. The structural models are cubic supercells, periodically repeated, ranging in size from 216 to 4096 atoms. In the analysis, we employ only q-vectors that are consistent with the boundary conditions used to obtain the modes. Upon averaging over q-vector direction, systematic dependences result. Partly through this analysis, a single resonant mode at a frequency near the cutoff of the (approximately) transverse acoustic modes has been detected in at least one of our models. The structural aspects of the models will also be discussed. In particular, no unusual structural ordering has been detected in the radial distribution function for the 4096-atom model.

Title: FY96 NRL DoD High Performance Computing Modernization Program Annual Reports
Author(s): Jean E. Osburn
E-mail Address: osburn@bohr.nrl.navy.mil
Citation: Naval Research Laboratory Publication NRL/PU/5590--97-329
Date: March 14, 1997
Report No.: CCS-97-003

Abstract

These reports summarize the accomplishments of the NRL Principal Investigators who received computer allocations on the DoD High Performance Computing Modernization Program Shared Resource Centers in FY96.

1996 PUBLICATIONS:

CCS-96-002 Visualizing Time-Dependent Particle Traces in the Context of Real-Time Visualization Environment, *Upul R. Obeysekare, Femando Grinstein, and Gopal Patnaik*

CCS-96-003 Virtual Workbench--A Non-Immersive Virtual Environment for Visualizing and Interacting with 3D Objects for Scientific Visualization, *Upul R. Obeysekare, Charles J. Williams, Jim Durbin, Larry Rosenblum, Robert Rosenberg, Fernando Grinstein, Ravi Rammamurti, Alexandra Landsberg, and William Sandberg*

CCS-96-004 Article for the DOD High Performance Computing Modernization Plan Requirements Survey Team, *Jean E. Osburn*

CCS-96-005 Real-Time Visualization of Numerically Simulated Jet Flows Using NASA/NAS'S Live, *Upul R. Obeysekare, Fernando Grinstein, and GopalPatnaik*

CCS-96-006 Visualizing Time-Dependent Particle Traces in the Context of Real-Time Visualization Environment, *Upul R. Obeysekare, Fernando Grinstein, and Gopal Patnaik*

CCS-96-007 Interactive Desktop Laboratory With Visual Supercomputing, *Upul Obeysekare, Fernando Grinstein, and Gopal Patnaik*

CCS-96-008 A 4096 Atom Model of Amorphous Silicon: Structure and Dynamics, *Brian Davidson, Joseph L. Feldman, Scott R. Bickham, and Frederick Wooten*

1995 PUBLICATIONS

CCS-95-001 An Application for Visualizing Molecular Dynamics Data Developed Under AVS/Express, *Upul R. Obeysekare and Chas J. Williams*

CCS-95-002 CM-5 Kernel Optimization of a Global Weather Model, *P.B. Anderson, D.W. Norton, and M.A. Young*